DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

OSWALDO ALEJANDRO TORRES DIAZ
DANNY JUAN PABLO LÓPEZ RODRIGUEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

OSWALDO ALEJANDRO TORRES DIAZ 79730882
DANNY JUAN PABLO LÓPEZ RODRIGUEZ 80791860

Trabajo de grado para optar al título de
Especialista en Seguridad Informática

Profesor: Ing. Álvaro Escobar Escobar
Ingeniero de Sistemas
Director Especialización Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

Nota de aceptación:

Aprobado por los jurados de grado
cumpliendo con los requisitos
exigidos por la Universidad Piloto
de Colombia para optar al título de
especialista en seguridad informática

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., septiembre 2017

DEDICATORIA

El presente trabajo es dedicado a nuestras familias, quienes han sido parte fundamental para el desarrollo de este proyecto, ellos son quienes nos dieron grandes enseñanzas y los principales protagonistas de este nuevo logro en nuestras vidas.

AGRADECIMIENTOS

El presente documento de trabajo de grado merece nuestros profundos agradecimientos a los directivos de Promociones y Cobranzas Beta por todo su apoyo y disposición durante la ejecución del proyecto.

Por supuesto no podemos dejar de agradecerle a mis compañeros de carrera, con quiénes compartí muchos momentos importantes, quiénes emprendieron este viaje conmigo y hoy nos encontramos departiendo anécdotas de esta experiencia vivida.

Al profesor Álvaro Escobar, quien gracias a su apoyo hizo posible la realización de este proyecto.

A nuestros padres, porque gracias a ellos quienes fueron los que nos formaron, para que hoy en día seamos las personas que somos.

CONTENIDO

pág.

INTRODUCCIÓN 20

1. DEFINICIÓN DEL PROBLEMA 23

2. JUSTIFICACIÓN 24

3. ALCANCE 25

4. OBJETIVOS 26

5. MARCO DE REFERENCIA 27

5.1. MARCO TEÓRICO. 27

5.2. MARCO HISTÓRICO 38

5.3. MARCO CONCEPTUAL 45

5.4. MARCO LEGAL 49

6. METODOLOGÍA 54

7. FASE 1 - RECONOCIMIENTO, RECOLECCIÓN, Y ANÁLISIS DE INFORMACIÓN 55

7.1 POBLACIÓN 55

7.2 RECOLECCIÓN DE INFORMACIÓN Y FUENTES 55

7.3 EJECUCIÓN PRUEBAS DE INGENIERÍA SOCIAL - FASE 1 58

7.4 PRUEBAS DE INGENIERÍA SOCIAL FASE 1 A PROMOCIONES Y COBRANZAS BETA 59

7.5 ANÁLISIS PRUEBAS DE INGENIERÍA SOCIAL - FASE 1.....65

7.6 ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 1.85

7.7 ANÁLISIS ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 1 88

8. FASE 2 – EJECUCIÓN PLAN DE CONCIENTIZACIÓN 94

8.1 ¿QUÉ SE BUSCA CON ESTE PLAN CONCIENTIZACIÓN? 94

8.2 ALCANCE.....94

8.3 CAPACITACIÓN.....95

8.4 CONTINUIDAD Y RECORDACIÓN.....98

8.5 RECOMENDACIONES DE GOBIERNO Y CONTINUIDAD.....103

9. FASE 3 - ANÁLISIS ESTADO LUEGO DE EJECUTAR EL PLAN DE CONCIENTIZACIÓN.....105

9.1 ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 3 105

9.2 ANÁLISIS ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 3 108

9.3 DEFINICIÓN PRUEBAS INGENIERÍA SOCIAL FASE 3. 119

9.4 ANÁLISIS PRUEBAS DE INGENIERÍA SOCIAL - FASE 3.....123

10. BUENAS PRÁCTICAS Y TIPS PARA IDENTIFICAR POSIBLES ATAQUES DE INGENIERÍA SOCIAL EN EL ÁMBITO TECNOLÓGICO, NEUROLINGÜÍSTICO Y PSICOLÓGICO.....131

10.1 ¿QUÉ HACER FRENTE A UNA SUPLANTACIÓN DE IDENTIDAD? 132

10.2 PHISHING.....132

10.3 DUMPSTER DIVING 133

10.4 REDES SOCIALES 134

10.5 SOFTWARE MALICIOSO MEDIANTE BAITING 134

10.6 SEGUIR PROTOCOLOS DE SEGURIDAD 135

11. CONCLUSIONES 137

BIBLIOGRAFÍA 139

ANEXOS 146

LISTA DE ILUSTRACIONES

Pág.

Ilustración 1. Pilares o principios de Seguridad Informática. 28

Ilustración 2. Objetivo organizacional. 48

Ilustración 3. Líneas de negocio. 49

Ilustración 4. Fórmula muestreo. 56

Ilustración 5. Documentos hallados en bandejas de reciclado 71

Ilustración 6. Documentos hallados en papeleras de basura 72

Ilustración 7. Consola herramienta SET creación de payload 74

Ilustración 8. Captura camweb_snap 75

Ilustración 9. Pantallazos de Facebook, perfil falso atacante y perfil víctima empleado de PYCB 84

Ilustración 10. Pregunta 1 encuesta fase 1. 85

Ilustración 11. Pregunta 2 encuesta fase 1. 86

Ilustración 12. Pregunta 3 encuesta fase 1. 86

Ilustración 13. Pregunta 4 encuesta fase 1. 86

Ilustración 14. Pregunta 5 encuesta fase 1. 87

Ilustración 15. Pregunta 6 encuesta fase 1. 87

Ilustración 16. Pregunta 7 encuesta fase 1. 87

Ilustración 17. Video ingeniería social Promociones y Cobranzas Beta 97

Ilustración 18. Correo 1. alerta de pretexting. 99

Ilustración 19. Correo 2. alerta de dumpster diving 99

Ilustración 20. Correo 3. alerta de phising 100
Ilustración 21. Correo 4. alerta de shoulder surfing 100
Ilustración 22. Correo 5. alerta de tailgating. 101
Ilustración 23. Afiche 1.....102
Ilustración 24. Afiche 2.....103
Ilustración 25. Preguntas 1 y 2 fase 3 Moodle. 105
Ilustración 26. Preguntas 3 y 4 fase 3 Moodle. 106
Ilustración 27. Preguntas 5 y 6 fase 3 Moodle. 106
Ilustración 28. Preguntas 7 y 8 fase 3 Moodle. 107
Ilustración 29. Preguntas 9 y 10 fase 3 Moodle. 107
Ilustración 30. Herramienta SET clonación de sitio web. 124
Ilustración 31. Ataque phishing captura usuario y contraseña. 124
Ilustración 32. Picadoras de papel. 127
Ilustración 33. Canecas reciclables de colores. 127

LISTA DE GRÁFICAS

Pág.

Gráfica 1. Pregunta 1 fase 88

Gráfica 2.Pregunta 2 fase 1 89

Gráfica 3. Pregunta 3 fase 1 90

Gráfica 4. Pregunta 4 fase 1 91

Gráfica 5. Pregunta 5 fase 1 92

Gráfica 6. Pregunta 6 fase 1 92

Gráfica 7. Pregunta 7 fase 1 93

Gráfica 8. Pregunta 1 fase 3 109

Gráfica 9. Pregunta 2 fase 3. 110

Gráfica 10. Pregunta 3 fase 3. 111

Gráfica 11. Pregunta 4 fase 3. 112

Gráfica 12. Pregunta 5 fase 3. 113

Gráfica 13. Pregunta 6 fase 3. 114

Gráfica 14. Pregunta 7 fase 3. 115

Gráfica 15. Pregunta 8 fase 3. 116

Gráfica 16. Pregunta 9 fase 3. 117

Gráfica 17. Pregunta 10 fase3. 118

Gráfica 18. Pregunta 11 fase 3. 119

LISTA DE CUADROS

Pág.

Cuadro 1. Objetivos Phishing....60
Cuadro 2. Usuarios objetivos baiting 61
Cuadro 3. Áreas objetivas baiting 61
Cuadro 4. Personal objetivo de pretexting 62
Cuadro 5. Áreas objetivo de pretexting....62
Cuadro 6. Áreas objetivo dumpster diving 63
Cuadro 7. Objetivos shoulder surfing....63
Cuadro 8. Objetivos Ingeniería Social en redes sociales....64
Cuadro 9. Pérdida del Caller id original desde una línea externa 67
Cuadro 10. Divulgación de entrada y salida de personal a la empresa 68
Cuadro 11. Falta de capacitación del personal en ataques de Ingeniería Social...68
Cuadro 12. Demora proceso aviso deshabilitación de usuarios 69
Cuadro 13. No cumplimiento de procedimientos de control de usuarios 70
Cuadro 14. Falta de control en el manejo de la información....73
Cuadro 15. Inexistencia de una catalogación correcta de la información 73
Cuadro 16. Usuarios con más permisos en red interna de los necesarios 75
Cuadro 17. Usuarios con permisos de acceso a internet sin ser necesarios....75
Cuadro 18. Demasiados administradores en el Controlador de Dominio 76
Cuadro 19. Administración de configuración de perfiles de usuarios del CD.....76
Cuadro 20. Listado víctimas Phishing....77

Cuadro 21. Desconocimiento del personal sobre este tipo de ataques 78

Cuadro 22. Desconocimiento del que hacer con emails que contienen phishing ..78

Cuadro 23. Mal uso de la cuenta corporativa de correo electrónico 78

Cuadro 24. Inexistencia de definición de uso de correo empresarial en Internet...80

Cuadro 25. Inexistencia de una herramienta que controles la fuga de información 80

Cuadro 26. Inexistencia de certificados de seguridad.....80

Cuadro 27. Uso inadecuado de las herramientas informáticas.....80

Cuadro 28. Inexistencia de configuración y política de intentos fallidos de contraseña 81

Cuadro 29. No cumplimiento en las políticas de seguridad informática.....81

Cuadro 30. Definición de tiempo de bloqueo de pantalla por inactividad.....81

Cuadro 31. Definición de des logueo o bloqueo de aplicativos por inactividad.....82

Cuadro 32. Desconocimiento de la importancia de bloquear el equipo y des autenticarse de aplicaciones.....82

Cuadro 33. Responsabilidad de invitados por parte del personal de la empresa ..83

Cuadro 34. Falta de verificación de contactos 84

Cuadro 35 Objetivos Phishing.....120

Cuadro 36. Áreas objetivas baiting 120

Cuadro 37. Personal objetivo de pretexting 121

Cuadro 38. Áreas objetivo de pretexting.....121

Cuadro 39. Áreas objetivo dumpster diving 122

Cuadro 40. Objetivos shoulder surfing.....123

LISTA DE ANEXOS

Pág.

Anexo A. Acta de reunión 1 146

Anexo B. Acta de reunión 2 151

Anexo C. Acta de reunión 3 155

Anexo D. Acuerdo de confidencialidad 158

Anexo E. Get out of jail 159

Anexo F. Documentos entregados por Promociones y Cobranzas Beta 160

Anexo G. Listas de asistencia.....168

Anexo H. Manual presentación concientización ingeniería Social Beta.....188

GLOSARIO

AMENAZA: una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS)[1].

ANTISPAM: es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel[1].

ANTIVIRUS: es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles[1].

APLICACIONES MALICIOSAS: las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware[1].

ATAQUES WEB: un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta[1].

CIBERDELITO: el ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. Este puede ocurrir en la computadora o en otros lugares[1].

CSIRT: (CSIRT por las siglas de Computer Security Incident Response Team). Es un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas[1].

ENCRIPTACIÓN: es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el

[1] Symantec, Glosario de Seguridad 101, Latino América, sin fecha de actualización, consultado el 18 de Agosto de 2016, [en línea], disponible en Internet: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

malware utiliza la encriptación para ocultarse del software de seguridad, es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo[1].

FIREWALL: un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles[1].

INGENIERÍA SOCIAL: método utilizado por los atacantes para engañar a los usuarios informáticos para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social[1].

KEYLOGGER: un keylogger (derivado del inglés: key "tecla" y logger "registrador" – "registrador de teclas") es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado para posteriormente memorizarlas en un fichero o enviarlas a través de internet[1].

MALWARE: el malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías[1].

OSINT: el acrónimo anglosajón OSINT se refiere Open Source Intelligence o Inteligencia de fuentes abiertas. Las fuentes de información OSINT, es un término acuñado y muy empleado entre militares, fuerzas del orden y personal de inteligencia de las agencias gubernamentales[1].

PAYLOAD: en virus informáticos, el payload es la carga dañina de un virus, es decir, la parte que realiza la acción maliciosa. El resto del código son las formas de distribuirse y camuflarse, por ejemplo: payload puede hacer referencia a los resultados dañinos que genera ese código malicioso[2].

---

[1] Symantec, Glosario de Seguridad 101, Latino América, sin fecha de actualización, consultado el 18 de Agosto de 2016, [en línea], disponible en Internet: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

[2] Alegsa, DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA**,** Latino América, sin fecha de actualización, consultado el 07 de Julio de 2016, [en línea], disponible en Internet: http://www.alegsa.com.ar.

PHISHING: el phishing es un método que los ciberdelincuentes utilizan para engañar y conseguir que sea revelada información personal como contraseñas, datos de tarjetas de crédito y de seguridad social o números de cuentas bancarias. Este es realizado mediante el envío de correos electrónicos fraudulentos o dirigiendo a la víctima a un sitio web falso[1].

PNL: la Programación Neurolingüística (PNL) es un modelo de comunicación conformado por una serie de técnicas cuyo aprendizaje y práctica están enfocados al desarrollo humano[3].

PSYOP: actividades psicológicas planeadas realizadas en paz y en guerra, dirigidas a audiencias enemigas, amigas y neutrales para influir en actitudes y conductas concernientes a la consecución de objetivos políticos y militares[4].

RANSOMWARE: (del inglés *ransom*, "rescate", y *ware*, por *software*) es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción[5].

RAPPORT: es la sintonía psicológica entre el terapeuta y paciente que permite la colaboración necesaria entre ambos. Sus dos pilares fundamentales son la mutua confianza y la comunicación fluida[6].

TIP: es un término inglés que puede traducirse como "consejo" o "sugerencia". Los tips, por lo tanto, son recomendaciones que se hacen respecto a un tema[1].

VECTOR DE ATAQUE: un vector de ataque es el método que utiliza una amenaza para atacar un sistema[1].

VIRUS: programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

---

[1] Symantec, Glosario de Seguridad 101, Latino América, sin fecha de actualización, consultado el 18 de Agosto de 2016, [en línea], disponible en Internet: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[3] Programacion-neurolinguistica, Latino América, sin fecha de actualización, consultado 23 de junio de 2017, [en línea], disponible en internet: https://psicologiaymente.net/vida/programacion-neurolinguistica#

[4] Biblioteca pleyades, operaciones psicológicas de guerra, Latino América, sin fecha de actualización, consultado el 15 de enero de 2017, [en línea] disponible en internet: https://www.bibliotecapleyades.net/sociopolitica/esp_sociopol_mindcon85.htm

[5] Panda security ¿Qué es un Ransom ware?, Latino América, sin fecha de actualización, consultado el 05 de marzo de 2018, [en línea], disponible en: http://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

[6] Psicoterapeutas, ¿Qué es el Rapport?, marzo 10 de 2010, Editado por la Dra. Moya Guirao, consultado el 08 de agosto de 2017, disponible en: http://psicoterapeutas.eu/rapport/.

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales[1].

VULNERABILIDAD: una vulnerabilidad es un estado viciado en un sistema informático o conjunto de sistemas que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio[1].

Otra definición, de Vulnerabilidad, consiste en una debilidad que puede proporcionar a un atacante el medio para acceder sin autorización a los activos de información[7].

[1] Symantec, Glosario de Seguridad 101, Latino América, sin fecha de actualización, consultado el 18 de Agosto de 2016, [en línea], disponible en Internet: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.

[7] Ministerio de Defensa Nacional Colombiano, Policía Nacional, RESOLUCIÓN 03049 DEL 24 de agosto de 2012, "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", ARTÍCULO 5. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN.

RESUMEN

Actualmente la información representa uno de los activos más importantes para las empresas, gracias a esta es posible tomar decisiones y generar estrategias para aumentar los ingresos económicos. Sin embargo, la información no solo puede ser usada para actividades empresariales o de conocimiento personal, sino que en algunos otros casos personas con intensiones delictivas pueden usarla para aprovecharse de la condición humana de siempre querer ayudar, motivo por el cual el uso de la información desde una perspectiva delictiva busca engañar a otros individuos para que estos realicen actividades sin estar conscientes de ellas y entregar datos o información sensible lo cual representa una falencia de seguridad en el mundo tanto a nivel personal como a nivel empresarial.

Es así como la ingeniería social, toma fuerza al momento de facilitar un ataque a nivel informático; gracias a esta es posible reducir los tiempos en hacer un ciberataque y garantizar que sea exitoso. Este método de ataque poco convencional se basa en engañar y manipular a las víctimas buscando obtener algún tipo de dato o información que sirva o ayude a garantizar un ataque informático más robusto donde el atacante obtenga un beneficio. Debido a esta, muchas empresas son víctimas de ataques a su personal mediante técnicas que involucran a sus empleados y no a sus recursos tecnológicos e informáticos, siendo así el colaborador una brecha de seguridad de la información más para las empresas y como se dice en el medio informático “el eslabón más débil de la cadena”.

Este proyecto abarca investigación de aspectos de técnicas utilizadas, aclaración de términos y conceptos de la temática, historia e información legal referente a la ingeniería social. Además, enfatiza su ejecución en la concientización del personal de la empresa Promociones y Cobranzas Beta S.A frente a esta problemática; para ello se realiza una evaluación y medición al estado de conocimiento y preparación frente a ataques de este tipo en una primera etapa; luego una concientización del personal de la compañía basada en un plan educativo que involucra capacitación y recordación sobre el tema como segunda fase y finalmente en una tercera etapa se realiza nuevamente una evaluación y medición del estado adquirido luego de la ejecución del plan de concientización. Luego de analizar y tabular la información obtenida de las tres fases ejecutadas, se entregan conclusiones de las actividades realizadas, recomendaciones a seguir acordes a los resultados obtenidos buscando corregir falencias encontradas y permitiendo así que la compañía Promociones y Cobranzas Beta S.A. genere una cultura de seguridad de la información y buenas prácticas a nivel laboral y personal.

Palabras Clave: Ingeniería Social, Ciberataque, Seguridad de la información

INTRODUCCIÓN

En el momento de usar la tecnología para manipular la información y las comunicaciones, se presentan retos y cambios continuos. A su vez esta se vuelve uno de los principales factores para manejar la información. Motivo por el cual dichas novedades o avances de la misma incrementan su uso con objetivos delictivos a nivel mundial.

Este motivo representa una amenaza en la seguridad de la información, según la política de defensa y seguridad establecida en el territorio colombiano por el Ministerio de Defensa: "En el caso de la seguridad en el espacio cibernético, el rápido crecimiento de las tecnologías de la información y las comunicaciones no sólo ha permitido aumentar la conectividad global, sino que también las amenazas sobre la seguridad en el ciberespacio se han incrementado. Estas amenazas se materializan principalmente en conductas delictivas dirigidas a afectar el patrimonio económico y la intimidad de las personas"[8]. Con el aumento, innovación y evolución permanente de los ataques cibernéticos y a su vez de la interconexión de tecnologías de la computación e información (Convergencia Tecnológica)[9], se hacen notoria la necesidad de acoger controles y medidas que permitan proteger a las personas y empresas frente a nuevas amenazas que puedan presentarse[10].

En gran parte los ataques tecnológicos son basados o planeados mediante la ingeniería social; cuando se habla de esta se tienen diferentes puntos de vista frente al significado y el funcionamiento de la misma en la sociedad; lo cual ha llevado a que dicha actividad sea sencillamente tomada como mentir; en otros casos es el uso de herramientas y artimañas por parte de estafadores, o en algunos otros es visto como un arte dado a los profesionales a fin de que estos cuentan con la posibilidad de usar algún tipo de truco frente a la mente humana; en sí, existen diferentes formas de pensar según las experiencias vividas. Sin embargo, como indica Christopher Hadnagy, "una definición de ingeniería social, es el acto de manipular a una persona a tomar una acción que puede o no estar

[8] Ministerio de defensa de la Republica de Colombia, "Política de defensa y seguridad", 2015, disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Descargables/espanol/politica_defensa_deguridad2015.pdf, consultado el 18 de mayo de 2017.

[9] "Es la tendencia para que diversos sistemas tecnológicos se desarrollen hacia la ejecución de tareas similares. La convergencia puede referirse a las tecnologías previamente separadas tales como voz (y características de la telefonía), datos (y usos de la productividad) y vídeo que ahora comparten recursos y obran recíprocamente" (Jenkins, Henry (2006) Convergence Culture, New York University Press, New York)

[10] Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. (ISO/IEC 13335-1:2004).

en el interés del objetivo, lo cual puede incluir en la obtención de información, acceso o conseguir que el objetivo realice ciertas acciones"[11].

De igual manera se encuentran muchas definiciones similares de expertos en seguridad informática en donde se concluye que la seguridad informática tiene como fin explotar la conducta humana y aprovechar la buena fe y confianza de las personas.

Dado que se presenta una problemática a nivel empresarial en donde posibles atacantes pueden aprovecharse de las personas usando diferentes técnicas de ingeniería social con el fin de obtener información confidencial de las empresas o disponer de alguna otra que le permita acceder a dicha información confidencial buscando obtener un beneficio; este proyecto diseña un plan de concientización que ayuda a hacer frente a la ingeniería social y a su vez se implementa en la empresa Promociones y Cobranzas Beta S.A. entregando información a los empleados de ataques de esta índole y dándoles a conocer cómo pueden ser posibles víctimas de ellos.

Este plan de concientización ayuda a los usuarios internos de la compañía Promociones y Cobranzas Beta S.A. a conocer los diferentes tipos de ataques de ingeniería social a los que pueden estar expuestos y así mismo disponer de un conocimiento básico sobre el tema, el cual a pesar de depender de cada persona y su aprendizaje les puede permitir mejorar en el uso de su perspicacia y así mismo facilitarse el ser capaces de detectar ciertos indicios que permitan identificar posibles ataques de ingeniería social.

Para ello, en una primera etapa se realizan pruebas de ingeniería social fundamentadas según el marco referencial de trabajo de social Engineering Framework; con dichas pruebas se identifican ciertas vulnerabilidades que no son explotadas y en las que se procura no manipular información confidencial de Promociones y Cobranzas Beta S.A., es importante recalcar que información confidencial que se pueda llegar a obtener no es expuesta como evidencia en este documento aunque es mencionada; no obstante dicha información es entregada a Promociones y Cobranzas Beta S.A. para que se tomen correctivos basados en las recomendaciones según el plan de concientización.

[11] Hadnagy Christopher, "Social Engineering the art of human hacking", Chapter 1. Editorial Wiley Publishing inc. 2011, p 23 – 31

En la segunda etapa se realiza el análisis de las vulnerabilidades encontradas; basándose en los resultados del análisis se estructurará el plan de concientización el cual se apoya en correos electrónicos, charlas, y talleres.

En la tercera etapa se realizan nuevamente pruebas de ingeniería social, análisis de vulnerabilidades e informe final en donde se indican los resultados obtenido con el respectivo planteamiento de continuidad de la estrategia de concientización frente a posibles ataques de ingeniería social.

1. DEFINICIÓN DEL PROBLEMA

Para Promociones y Cobranzas Beta S.A resulta pertinente contar con un plan de concientización frente a la amenaza de la ingeniería social, para ello es necesario sensibilizar a los usuarios de la empresa sobre esta temática; también es importante que los empleados comprendan el valor de los datos e información que manejan y como estos pueden ser usados para realizar otros ataques si son capturados por atacantes informáticos.

Con lo anterior, es necesario responder la siguiente pregunta:

¿Cómo podrían prepararse los empleados de Promociones y Cobranzas Beta S.A. para identificar un ataque de ingeniería social?

2. JUSTIFICACIÓN

La palabra “hackers” comúnmente es relacionada con medios informáticos y tecnológicos, además de ejecución de scripts, ataques y penetración en la red; pero no siempre los ataques son a nivel tecnológico (hardware o software) directamente, hay otro tipo de ataques que en pocas oportunidades son tenidos en cuenta, como es el caso de la ingeniería social, la cual a pesar de no ser contemplada por la mayoría de personas y empresas es una técnica o forma de explotar limitantes de las personas y mediante diversos métodos sustraer información usando como medio principal la interacción social; de este modo la persona que es vulnerada no se da cuenta de cómo o cuándo entrega los datos o información necesaria para terminar siendo víctima de un ataque informático. Esta práctica recurre principalmente a la manipulación de la psicología humana mediante el engaño, el cual, aunque no siempre de parte del atacante, existe un conocimiento profundo de las ciencias socio humanísticas, esté obra según la premisa de: en la cadena de seguridad de la información el ser humano es el eslabón más débil.

Mencionado lo anterior y siendo la información uno de los activos más importante con el cual pueden cometerse fraudes o accesos no autorizados es imprescindible ahondar en el estudio de la técnica de ingeniería social enfocada al hacking la cual podría acabar con cualquier esfuerzo puesto sobre los controles tecnológicos en pro de la seguridad, ya que esta técnica es un modo de operación silencioso con el cual en muchas ocasiones las víctimas nunca se percatan de haber sido objeto de esta hasta el momento en el que son informados y una vez adquirida la experiencia o el aprendizaje se adquiere una capacidad en la que la lógica básica y perspicacia de las víctimas ayuda a que a estas cuenten con una alarma frente a la detección de ciertos indicios o tips que permiten identificar un ataque de ingeniería social.

Para Promociones y Cobranzas Beta S.A, resulta pertinente contar con un plan de concientización frente a la amenaza expuesta, para ello es necesario sensibilizar a los usuarios de la empresa en la importancia de dar uso adecuado a los medios tecnológicos al igual que los datos e información, ya que al generar conciencia sobre dicho uso esta les permitirá contar con un conocimiento general el cual los orientará en la importancia de identificar posibles ataques a los que puedan llegar a estar expuestos frente a esta técnica de hacking.

3. ALCANCE

Se pretende establecer un punto de partida en el estudio de la ingeniería social al ser introducida en ambientes activos con alto grado de confidencialidad. Dicho punto abarca una encuesta y pruebas de ingeniería social para identificar los temas a profundizar en el plan de concientización; las pruebas están basadas en la metodología de OSSTMM versión 3.0 Vulnerability Assessment, la cual sólo contempla encontrar vulnerabilidades sin ser explotadas; en la etapa dos, de acuerdo a los resultados obtenidos se diseña el plan de concientización frente a la problemática expuesta y se pone en ejecución buscando que los empleados de Promociones y Cobranzas Beta adquieran un conocimiento básico intuitivo el cual les permita identificar posibles ataques de esta índole; en la tercera etapa se realizan pruebas, análisis y resultados de verificación para evaluar a los empleados y comparar los resultados obtenidos en cada una de las etapas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar e implementar un plan de concientización de ingeniería social, el cual entregue conocimientos generales sobre la ingeniería social para los trabajadores de Promociones y cobranzas Beta S.A.

4.2 OBJETIVOS ESPECÍFICOS

- Analizar los posibles escenarios en los cuales los empleados de Promociones y Cobranzas Beta S.A podrían ser víctimas de ataques de ingeniería social.

- Realizar una encuesta y prueba de ingeniería social, antes y después de generar el plan de concientización, para evaluar el estado actual y posterior a la concientización frente al ser víctima de un ataque de ingeniería social de los usuarios internos de Promociones y Cobranzas Beta S.A

- Sugerir continuidad en la concientización, buenas prácticas y tips, en donde se puedan identificar posibles ataques de ingeniería social en el ámbito tecnológico, neuro lingüístico y psicológico.

5. MARCO DE REFERENCIA

5.1. MARCO TEÓRICO.

El enfoque principal de este proyecto es la concientización sobre los posibles ataques de ingeniería social a los que pueden estar expuestos los empleados de Promociones y Cobranzas Beta S.A., por lo cual es necesario mostrar definiciones y técnicas referentes a la temática desde distintos puntos de vista al igual que enfoques teóricos; con esto se busca comprender y profundizar en la ingeniería social y cómo está relacionada directamente con la seguridad informática y la ciberdelincuencia.

5.1.1 ¿Qué es la seguridad informática? La Resolución 03049 del 24 de agosto de 2012 del Ministerio de Defensa Nacional Colombiano la define como: "la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma"[12].

El U.S. National Information Systems Security Glossary, define a los sistemas de información de seguridad como: la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el almacenamiento, procesamiento o tránsito de la misma y contra; la denegación de servicios a usuarios autorizados, o la prestación de servicios a usuarios no autorizados, incluyendo las medidas necesarias para detectar, documentar y contrarrestar tales amenazas[13].

Tres elementos ampliamente aceptados de seguridad de la información son:

- Confidencialidad
- Integridad
- Disponibilidad

En la Ilustración 1. Pilares o principios de seguridad informática, podemos observar una imagen que muestra los tres pilares de la seguridad de la información

[12] Ministerio de Defensa Nacional Colombiano, Policía Nacional, RESOLUCIÓN 03049 del 24 de agosto de 2012, "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", ARTÍCULO 5. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN.

[13] Universidad de Nevada, Las Vegas, "Definition of Information Security", 2015, disponible en: https://oit.unlv.edu/network-and-security/definition-information-security, consultado el 18 de mayo de 2017.

Ilustración 1. Pilares o principios de Seguridad Informática

Fuente: GÓMEZ, Álvaro. Enciclopedia de la seguridad informática. 2 Ed. Alfa Omega, 2011. Pág. 5.

En la norma técnica ISO/IEC 27000:2014[14] se define el propósito de la seguridad de la información como: proteger y preservar la confidencialidad, integridad y disponibilidad de información. También puede proteger y preservar la autenticidad y la fiabilidad de la información, además de garantizar que las entidades puedan rendir cuentas[8].

5.1.2 Principios de la seguridad informática. El principal fin de un sistema de seguridad de la información se basa en brindar tres principios, la disponibilidad, integridad y confidencialidad, para la información institucional, como lo podemos observar en la Ilustración 1. Pilares o principios de seguridad informática, estos se establecen de la siguiente manera:

5.1.2.1 Confidencialidad (Confidentiality). Para el Ministerio de Defensa Nacional Colombiano (MINDEFENSA) este término "Establece que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"[15].

También la norma técnica ISO/IEC 27000:2014[14] a su vez puede ser entendida como una característica que se aplica a la información para proteger y preservar confidencialidad, la misma significa para asegurarse de que no esté disponible o compartida con entidades no autorizadas. En este contexto, las entidades incluyen a las personas y procesos.

5.1.2.2 Integridad (Integrity). Acorde al MINDEFENSA "Consiste en salvaguardar la exactitud y estado completo de los activos de información, es decir que la información solo pueda ser modificada por personal autorizado"[15].

La norma técnica ISO IEC 27000 hace referencia a proteger la exactitud de la información y lo completa que esta se encuentra[8].

5.1.2.3 Disponibilidad (Availability). Según el MINDEFENSA "Establece que la información debe estar disponible para su uso en todo momento, para ser usada o vista solo por personal autorizado"[15].

También es entendida por la ISO IEC 27000, como una característica o propiedad de algo que se encuentra disponible, si es accesible y utilizable, cuando una entidad autorizada demanda acceder[14].

5.1.3 ¿Qué es ingeniería social? Merriam-Webster indica que existe una definición Simple "*the practice of making laws or using other methods to influence public opinion and solve social problems or improve social conditions" (traducción: la práctica de hacer leyes o el uso de otros métodos para influir en la opinión pública y resolver problemas sociales o mejorar las condiciones sociales) Y una definición completa "management of human beings in accordance with their place and function in society : applied social science*" (la gestión de los seres humanos en función de su lugar y su función en la sociedad: aplicado a las ciencias sociales)[16].

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) hace referencia en su sitio web, al término ingeniería social como un "método utilizado por los atacantes para engañar a los usuarios informáticos, para

[14] ISO/IEC 27000, Términos y definiciones, 2014, sección 2.
[15] Ministerio de Defensa Nacional Colombiano, Policía Nacional, RESOLUCIÓN 03049 del 24 de agosto de 2012, "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", ARTÍCULO 5. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN.
[16] Merriam-Webster, definición de ingeniería social, Enter, Editorial triple, sitio web Actualizado: viernes, 30 de septiembre de 2016. Disponible en: http://www.merriam-webster.com/dictionary/social+engineering, Consulta: Domingo, 02 de octubre de 2016.

que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social"[17].

La definición expuesta por Kevin Mitnick y William Simón, en su libro "the art of decepción", indica que: "La ingeniería social utiliza la manipulación, la influencia y el engaño para conseguir a una persona, una información privilegiada de confianza dentro de una organización, para cumplir con una petición, y la solicitud es por lo general para divulgar información o realizar algún tipo de elemento de acción que beneficie a que atacante. Podría ser algo tan sencillo como hablar por teléfono a algo tan complejo como conseguir un objetivo para visitar una Web, que explota una falla técnica y permite al hacker para hacerse cargo del equipo"[18].

Entrando a ver como algunos medios en Colombia dan a conocer en parte la ingeniería social, hay diferentes artículos, que hablan sobre esta:

Un ejemplo es de la revista Semana con el artículo "Conozca de qué se trata la ingeniería social y tome precauciones", en donde este se empieza con el siguiente párrafo: "Al final, detrás de la pantalla hay un humano, y no es una frase filosófica, pasa que, los atacantes se aprovechan de las emociones de los usuarios para acceder a la información de sus cuentas para instalar virus o robarlos"[19].

A su vez la emisora Caracol Radio con, "ingeniería social: el hackeo humano" entrevista realizada a Guillermo Santos, presidente de la revista Enter, en donde Santos cita a Kevin Mitnick y define ingeniería social como "el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales"[20].

Existen algunos otros artículos y noticias sobre este tema publicado en Colombia, en Latino América y en el mundo, haciendo un intento por dar a conocerla y enterar a las personas y empresas, de cómo es usada por ciberdelincuentes que buscan sacar provecho de estas técnicas y así lograr sus objetivos criminales.

---

[17] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, definición de Ingeniería social, Enter, Editorial triple, sitio web Actualizado: viernes, 30 de septiembre de 2016. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-18800.html, Consulta: Domingo, 02 de octubre de 2016.

[18] 11 K. Mitnick and W. Simon, The art of deception. Indianapolis: Wiley, 2002.

[19] Sin autor. Conozca de qué se trata la 'ingeniería social' y tome precauciones, Revista Semana, Publicaciones Semana S.A, Bogotá, 30 de enero de 2014. Disponible en: http://www.semana.com/tecnologia/tips/articulo/conozca-que-trata-ingenieria-social-tome-recauciones/373280-3, Consulta: miércoles, 03 de agosto de 2016.

[20] SANTOS, Guillermo, Ingeniería Social: el hackeo humano (entrevista), Caracol Radio, Bogotá, 31 de agosto de 2011. Disponible en: http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html, Consulta: miércoles, 03 de agosto de 2016.

5.1.4 Tendencias humanas de la ingeniería social. Según Kevin Mitnick, el más conocido ingeniero social a nivel mundial de la actualidad, la ingeniería social es basada en 6 tendencias humanas básicas[21]

- Autoridad
- Tendencia natural a ser útil o a ayudar
- Gusto y semejanza
- El movimiento alternativo
- El Compromiso y la consistencia
- Poca participación

"La ingeniería social se basa en la mentira y el ingenio de los usuarios comunes",[22] sobornos, mentiras y la seducción pueden ser usados para engañar a las personas, a empleados honestos y deshonestos, consiguiendo que estos faciliten datos privados o incluso acceso físico a algún lugar. Lo mejor es que es uno de los más baratos y más eficaces ataques, a menudo no técnicos utilizados por los atacantes simplemente mediante la explotación de los seres humanos en lugar de debilidad tecnológica.

5.1.5 Tipos de ingenieros sociales. Cuando se habla de ingeniería social esta puede ser usada de muchas formas: de forma maliciosa para realizar un ataque informático, o conseguir información confidencial para luego obtener algo a cambio de esta, o sencillamente puede ser usada amablemente para obtener a cambio un favor, realmente existen miles de usos que se pueden dar a la ingeniería social. Acorde al contenido de este proyecto es importante observar brevemente las diferentes formas de ingenieros sociales y una breve descripción de cada uno de ellos.

Según el libro “Social Engineering: the art of human hacking”[24] los tipos de ingenieros sociales son:

5.1.5.1 Hackers. El término de "hacker" nació en los años 50s, con algunos técnicos de empresas telefónicas en Estados Unidos, que averiaban los dispositivos físicos para posteriormente repararlos. Su traducción literaria es “hachazo”, como golpear con un hacha, y se puede definir como: una persona

[21] K. Mitnick and W. Simon, The art of deception. Indianapolis: Wiley, 2002.
[22] M. Nohlberg, “Social engineering: understanding, measuring and protecting against attacks”, ph.d. Licenciature, dept. Hum. And inf., univ. Of skövde, Sweden, 2007.

informática la cual usa técnicas de acceso no programadas, para de esta manera poder ingresar a un sistema informático, con diversos objetivos[23].

Debido a que los piratas informáticos atacan al software y vectores de software mediante la piratería informática remota los proveedores de software son cada vez más hábiles en la creación de aplicaciones y hacen que estas sean más fuerte o más difíciles de penetrar motivo por el cual los ciberdelincuentes recurren con mayor frecuencia al uso de ingeniería social. A menudo, el uso de una mezcla de hardware y habilidades personales utilizando técnicas de esta índole en los principales ataques ayuda a que estos consigan su objetivo con menor grado de dificultad.[24]

Es importante resaltar que los hackers a menudo emplean técnicas de ingeniería social ya que el factor de debilidad humana se puede romper fácilmente a diferencia de penetrar en una red.[25]

5.1.5.2 Crackers. Es alguien que irrumpe en el sistema computarizado de otra persona sin el consentimiento de esta, comúnmente sobre una red; consiguiendo contraseñas o licencias de programas informáticos; o de otras maneras intencionales que buscan violar la seguridad informática.[26]

5.1.5.3 Penetration testers (probadores de penetración). Es una persona ofensiva por naturaleza, es decir que intenta aprovechar al máximo cualquier brecha de seguridad; ellos aprenden y utilizan las habilidades de los hackers hasta el punto de contar con las habilidades de un ciberdelincuente solo que usan estas para ayudar realmente a garantizar la seguridad de un cliente y nunca usan la información para beneficio personal o daño del objetivo[26].

Pueden utilizar suplantación de identidad u otras técnicas para capturar información de empleados confiados; comúnmente se capturan contraseñas, usuarios de entrada a sitios físicos u otro tipo de acceso a sistemas[27].

[23]AVILÉS GÓMEZ, Manuel, et al. Delitos y delincuentes: cómo son, cómo actúan. San Vicente, España: ECU, 2010. 404 p. ISBN 978–84–9948–151–7.

[24] HADNAGY, Christopher, Social Engineering: the art of human hacking, Wiley Publishing Inc., 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2011.

[25] Social-Engineer.org, Marco de referencia de ingeniería Social, Discusión general, los Hackers, Social Engineer, Inc.2016, consultado el 10 de agosto de 2016.

[26] Hansen Dennis, “SAVE Social Vulnerability & Assessment Framework”, Dennis Hansen (ed.) Royal Danish Defence College, febrero 2017, Glosario.

[27] Social-Engineer.org, Marco de referencia de ingeniería Social, Discusión general, los Hackers, Social Engineer, Inc.2016, consultado el 10 de agosto de 2016.

5.1.5.4 Espías. Usan la ingeniería social como una forma de vida. A menudo en el empleo de todos los aspectos del marco de esta temática son expertos. Espías de todo el mundo se enseñan diferentes métodos engañando víctimas y haciéndoles creer que son alguien o algo que no son. Muchas veces los espías también se basan en la credibilidad conociendo un poco o incluso mucho sobre el negocio o el gobierno.

5.1.5.5 Ladrones de identidad (identity thieves). El robo de identidad es el uso de la información personal como el nombre de alguien, números de cuentas bancarias, dirección, fecha de nacimiento y número de seguridad social sin el conocimiento del propietario; este delito puede variar de ponerse un uniforme para hacerse pasar por alguien a estafas mucho más elaboradas; los ladrones de identidad emplean muchos aspectos de la ingeniería social y con el paso del tiempo parece más fácil utilizar sus técnicas y son más indiferentes al sufrimiento que pueden llegar a causar.[28]

5.1.5.6 Empleados descontentos. Cuando empleado se encuentra insatisfecho, lo cual sucede a menudo, estos entran en una relación de confrontación con su empleador; normalmente esto puede ser una situación de un solo lado porque el empleado será quien tratará de ocultar su nivel de desagrado para no poner en riesgo su empleo; sin embargo, cuanto más descontento se encuentre un empleado más fácil será para justificar actos de robo, vandalismo, u otros delitos.[28]

5.1.5.7 Estafadores. Las estafas apelan a la codicia u otros principios que atraen a las creencias de la gente; los estafadores o timadores dominan la capacidad de leer a la gente y recoger a cabo pequeñas señales que hacen de una persona una buena marca u objetivo; también son hábiles en la creación de situaciones u oportunidades que se presentan como inmejorables a un objetivo.[28]

5.1.5.8 Reclutadores de ejecutivos. Reclutadores de ejecutivos o Head Hunters, como se les llama, solicitan personas para puestos de trabajo con las empresas; utilizan diversos recursos o herramientas para encontrar a las personas adecuadas para los requisitos de trabajo que los empleadores establecen. Por lo general los datos se reúnen y se ven a través de la hoja de vida y sitios en línea para encontrar el mejor perfil; ellos trabajan para una empresa de una comisión fuera de su salario potencial o se puede contratar directamente un cazatalentos de

[28] HADNAGY, Christopher, Social Engineering: the art of human hacking, publicado por Wiley Publishing Inc., 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2011.

una cuota, estos van a hacer casi cualquier cosa para que esto suceda; convertirse en su amigo, escuchar sus problemas, ofrecer promesas de encontrar una coincidencia en su trabajo ideal[29].

5.1.5.9 Vendedores. El personal de ventas a menudo utiliza pretextos para obtener información sobre su empresa y lo que están buscando;[29] los vendedores deben dominar las habilidades de muchas personas; muchos gurús de las ventas dicen que un buen vendedor no manipula a la gente, pero si utiliza sus habilidades para averiguar cuáles son las necesidades de las personas y luego ve si pueden suplir las mismas con sus ofertas. El arte de las ventas tiene muchas habilidades tales como la recopilación de información, la obtención, la influencia, los principios psicológicos, así como muchas otras habilidades sobre las personas.

5.1.5.10 Los gobiernos. No muy a menudo son mirados como ingenieros sociales; sin embargo, los gobiernos utilizan la ingeniería social para controlar los mensajes que liberan, así como las personas que gobiernan; muchos gobiernos utilizan la prueba social, la autoridad y la escasez para asegurarse de que sus temas están en control. Este tipo de técnica no siempre es negativa ya que algunos de los mensajes de retransmisión de estos son para el bien de la comunidad y el uso de ciertos elementos puede hacer que el mensaje sea más atractivo y ampliamente aceptado.

Al hablar de la ingeniería social en un gobierno el término adquiere un nuevo significado o por lo menos en un sentido mucho más amplio, ya que hace referencia a la manipulación de un grupo de personas a través de las leyes y principios a fin de decirles a las personas lo que es y no es aceptable dentro de la sociedad; esto no denota que todo es malo, es decir, una ley sobre el asesinato y el abuso infantil puede ser una protección para los ciudadanos[29].

5.1.5.11 Los médicos, psicólogos y abogados. A pesar de que no podrían parecer expertos en ingeniería social, las personas en estas carreras encajan en la misma categoría que muchos de estos otros ingenieros sociales; este grupo emplea los mismos métodos utilizados por los otros grupos en esta lista; y comúnmente deben utilizar la felicitación y la entrevista adecuada y tácticas de interrogatorio, si es que no todos los principios psicológicos de la ingeniería social para manipular sus objetivos (clientes) en la dirección que desean que realicen ciertas actividades o evidencien cierta información[24].

[29]Social-Engineer.org, Marco de referencia de ingeniería Social, Discusión general, los Hackers, Social Engineer, Inc.2016, consultado el 10 de agosto de 2016.

5.1.5.12 Personas en su día a día. Como se puede observar y sin importar el campo de acción la ingeniería social hace parte de muchos de los aspectos de nuestras vidas solo que no lo tenemos presente; probablemente en muchas situaciones del día a día como personas se presenta la ingeniería social y sin darse cuenta es usada, con el tiempo se aprende a utilizar esos elementos en donde entra en juego la habilidad, según las experiencias vividas se aplica esta de una manera u otra[29].

5.1.6 ¿Cúal es el motivo de usar ingeniería social? Un atacante o hacker tiene claro que puede tardar mucho tiempo tratando de conseguir una contraseña o información que le permita acceder de una u otra forma a información confidencial, lo cual puede cambiar o reducir en factor tiempo con una llamada y un pretexto en cuestión de minutos, o usar diversas técnicas como buscar y hablar con empleados descontentos, e incluso entregar regalos de medios de almacenamiento con un programa malicioso que le permita ingresar a una red; en realidad hay muchas técnicas o formas de usar la ingeniería social que facilitan el poder disponer de ingreso no autorizado o datos que brindan accesos a información confidencial.

El problema al intentar utilizar técnicas de ingeniería social es que no hay reglas exactas sobre cómo engañar a alguien todo depende de la imaginación y astucia para usarlas; no existe un método que funcione con todo el mundo y hay muchas técnicas que se pueden utilizar cuando se trata de convencer a alguien acerca de su identidad, pero en general cuando se habla de la ingeniería social hay problemas psicológicos a cambio de tecnológicos los cuales pueden ayudar a tener éxito en el ataque.[30]

Según el artículo publicado por la IEEE de T. Qin and J. K. Burgoon[31], la técnica más común es el ser muy amable y presentar algún tipo de autoridad, sin embargo, hay gran selección de materiales de influencia, que en cierta medida explican por qué y cómo los seres humanos reaccionan a ciertas técnicas de convencimiento.

Según The Social-Engineer Podcast durante los últimos años los incidentes de seguridad en los que se ven utilizadas técnicas de ingeniería social en casos de

[30] ElMundo.es "¿Cuánto puede tardar un 'hacker' en adivinar tu contraseña?", 09/02/2016, disponible en: http://www.elmundo.es/papel/todologia/2016/02/09/56b1fc68268e3e70488b4572.html, consultado el 10 de mayo de 2017

[31] T. Qin and J. K. Burgoon. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering, Univ. Of. Arizona, 2007.

fraude y violaciones de datos se han venido incrementando con el pasar del tiempo. Según informes dados a conocer por los líderes de la industria como lo son Sophos, Verizon, Kaspersky, entre otros, indican que las tácticas de ingeniería social como phishing, vishing y la suplantación de identidad son combinadas con otros métodos como la piratería digital para hacer de los ataques efectivos y rentables para los atacantes; la única manera de protegerse contra estos ataques es a través de la formación y la creación de cultura de seguridad; es de conocimiento de los atacantes que en muchas oportunidades los empleados no son conscientes de estar haciendo algo mal o del valor real de la información, esto sucede por ingenuidad creada en un ambiente perfecto para un quebrantamiento de seguridad.

5.1.7 Ataques de ingeniería social. Básicamente consiste en persuadir a una persona para generar cierta influencia en la ejecución de sus acciones; diciéndolo de otra forma, es manipular personas influenciándolas a que ejecuten acciones específicas sin ser conscientes de ser víctimas de un delito informático, para esto existen diferentes técnicas, métodos o formas utilizadas para conseguir dicho objetivo con las cuales el atacante busca generar una situación confiable y creíble. A continuación, se definen las técnicas más comunes y las usadas para este proyecto.

5.1.7.1 Phishing. Según la reconocida empresa de antivirus Kaspersky “Es una variedad de programas espías que se propaga a través de correo; buscan recibir los datos confidenciales del usuario, de carácter bancario preferiblemente. Los emails phishing están diseñados para parecer igual a la correspondencia legal enviada por organizaciones bancarias, o algunas marcas conocidas. Tales correos electrónicos contienen un enlace que direcciona al usuario a una página falsa idéntica a la genuina solicitando datos confidenciales, como el número de la tarjeta de crédito”[32].

En pocas palabras es un correo electrónico combinado con sitios maliciosos los cuales se hacen pasar por sitios confiables, en la mayoría de ataques buscan robar información confidencial de cuentas bancarias, credenciales de acceso o información almacenada en el equipo víctima.

5.1.7.2 Baiting. Es un tipo de ataque de ingeniería social el cual se basa en dejar medios magnéticos como USB, CD y DVD “olvidados” los cuales contienen

[32] Kasperski, Seguridad 101: Los tipos de malware, Kasperski Lab, actualizado el 10 de mayo de 2016. Disponible en: http://support.kaspersky.com/sp/viruses/general/614, Consultado: miércoles, 03 de agosto de 2016.

software malicioso; estos elementos se dejan en lugares claves los cuales pueden ser estacionamientos cerca del automóvil de la víctima, en escritorios de oficina, cafeterías entre otros para garantizar y asegurar que el ataque sea exitoso; este ataque se puede complementar realizado un perfilamiento del objetivo y así poder adicionar etiquetas a los medios magnéticos consiguiendo que estos sean más atractivos para la víctima; comúnmente el objetivo de este ataque es conseguir que los usuarios inserten dichos medios magnéticos en sus computadores o estaciones de trabajo y lograr infectar estos o abrir alguna puerta trasera con el fin de poderlos acceder remotamente y tomar el control.

En el libro “Social Engineering: the art of human hacking” se encuentra la siguiente definición: “Un ataque en persona, donde se accede a la construcción del objetivo u otra propiedad por algún método, normalmente se dejan caer o regalan dispositivos extraíbles como USB o DVD los cuales contienen archivos maliciosos embebidos o se encuentran infectados con código malicioso”[24].

5.1.7.3 Pretexting. Acorde al libro "The Social Engineering´s Play Book a practical guide to pretexting" esta es “una táctica o técnica en la que un ingeniero social se hace pasar como una persona de autoridad, normalmente se hace pasar por una persona de soporte técnico que necesita con urgencia el acceso al computador del usuario o más osado aun a la sala de servidores de una compañía con el fin de para arreglar algo”[33]

Especificando un poco más este ataque busca persuadir a la víctima para que entregue información confidencial de ella o de la empresa donde trabaja; este ataque tiene una forma de operar específica en la cual es necesario realizar una investigación sobre la víctima y sobre las áreas que interactúan con la misma para conocer y crear un libreto o guion que facilite y familiarice a la víctima, es conveniente tener listos datos como nombre completo, fecha de nacimiento, número de cédula, número de teléfono, entre otros, para brindar información a la víctima de modo que se cree un ambiente de confianza.

5.1.7.4 Dumpster diving O going through the garbage. Es un tipo de ataque de ingeniería social el cual se basa en buscar papeles, DVD, USB discos duros o documentos con información confidencial en la basura o en bandejas de papel reciclado, ya que a menudo se desechan documentos con información importante como números de cuenta, cartas de despido, papel membretado, etc.

[24] HADNAGY, Christopher, Social Engineering: the art of human hacking, publicado por Wiley Publishing Inc., 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2011.
[33] TALAMANTES, Jeremiah, The Social Engineering´s Play Book a practical guide to pretexting, Publicado por HexCode, 2014.

Según Hadnagy “dumpster diving puede ofrecer una manera rápida de encontrar toda la información que desea. Recuerde que algunos indicadores son clave a la hora de realizar una inmersión en una contenedora de basura”[24].

Según Hansen, dumpster diving en las tecnologías de información es una forma de buceo en contenedores de basura, esta técnica es utilizada para recuperar información que podría ser útil con fines de llevar a cabo un ataque dentro de una red informática. Esta no se limita a buscar en la basura información obvia como los códigos de acceso, contraseñas escritas en notas adhesivas, si no que cualquier información aparentemente inocente como una lista telefónica, calendario u organización, pueden utilizarse para ayudar a un atacante utilizando otras técnicas de ingeniería social, para complementar información que permita acceder a la red informática[18].

5.1.7.5 Vishing. Es un tipo de ataque de ingeniería social el cual se basa en llamadas telefónicas las cuales se pueden generar desde teléfonos convencionales, teléfonos celulares o voz IP, la finalidad de las llamadas es engañar a la persona que está al otro lado del teléfono para que suministre información confidencial, por lo general se suplanta a personal de empresas cercanas a la misma empresa o a personal de la misma empresa. Según el libro “the social engineer´s play book” vishing es un ataque de ingeniería social llevado a cabo por teléfono. Este método es utilizado por los atacantes para robar información bancaria presentándose como representante del banco mientras se le pide a la víctima validar su cuenta, dando información de la tarjeta de crédito por teléfono[33].

5.2. MARCO HISTÓRICO

5.2.1 Orígenes de la ingeniería social. La expresión ingeniería social inicio en 1894 en un ensayo del empresario y filántropo holandés J.C. Van Marken[34] el cual fue difundido por la integrante de Musée Social, Émile Cheysson, en Francia[35]. Dicho concepto tuvo un gran impulso en el libro “Social Engineering” escrito por W.H. Tolman, en Estados Unidos, W.H. Tolman fue conocido en su época debido a su trabajo para ayudar a las personas de bajos recursos. Gracias a dichos planteamientos los cuales se enfocaban en la inexistencia dentro de las empresas

[33] TALAMANTES, Jeremiah, The Social Engineering´s Play Book a practical guide to pretexting, Publicado por HexCode, 2014

[34] Nederlandsch Economisch-Historisch Archief: J.C. van Marken - Biografisch portret.

[35] Émile Cheysson es ingeniero y reformador social francés , nacido en Nimes (Gard) en18 de mayo de 1836y murió en Leysin (Suiza) el7 de febrero de 1910

de una función social, haciendo referencia a algo similar a los departamentos de recursos humanos hoy en día, buscando mejorar el trato entre personas dentro de una compañía; él preveía dar solución a problemas sociales permitiendo hacer énfasis en el carácter no técnico de profesional en ingeniería social; dicho contraste con el posterior uso de este término, el cual fue popularizado alrededor de 1911.

Por otro lado, George Parker a principios de 1900 utilizó una táctica de ingeniería social para vender a los turistas sitios famosos como el puente de Brooklyn, en 1920 Charles Ponzi estafó a inversores con la promesa de rendimientos increíbles[36] .

Básicamente el origen del término "ingeniería social" fue entendido por los pensadores liberales a mediados de siglo XIX[37]. Buscando crear "ingenieros sociales" como un grupo enfatizado en ser intermediarios racionales entre el trabajo y el capital. Sin embargo, el término dejó de ser usado para las décadas de los años 30s y 40s del siglo XX, según Carl Marklund[38].

Luego de este énfasis se generalizó la percepción de la "ingeniería social" la cual puede ser usada como método o técnica para conseguir diferentes resultados a nivel social y dejo de ser usada para dar solución a problemas sociales y se convirtió en una técnica para manipular a las personas; haciendo visible que propagandas, campañas políticas y la misma religión entre muchas otras que pueden ser consideradas ingeniería social dado que buscan lograr un comportamiento específico en los seres humanos. En 1945 Karl Popper en el primer volumen de "la sociedad abierta y sus enemigos" reintroduce el término dando un sentido diferente y planteándolo como: implementación de métodos críticos y racionales de la ingeniería y ciencia a los problemas sociales[39].

La ingeniería social, la ciencia y arte de hackear seres humanos ha presentado alto incremento en su auge durante la última década debido al éxito de la comunicación de datos como son: correos electrónicos, redes sociales y diferentes formas de compartir la información de manera oportuna y prácticamente instantánea mediante la nube. En el sector de la seguridad de tecnologías de la información el término de ingeniería social se utiliza para hacer referencia a una serie de técnicas que usan los criminales para manipular sus víctimas con el fin de

[36] Talamantes, Jeremiah. The Social Engineer's Playbook: A Practical Guide to Pretexting (pp. 4-5). Hexcode Publishing. Edición de Kindle.
[37] New York Times: Dr. Tolman Sails on His Mission.
[38] Carl Marklund-2007: Some Notes on the Rhetorics of Social Engineering in Depression-Era Sweden and the USA
[39] CPU 2012 al 2014–Revista de Coordinación de Psicología del Uruguay, Relaciones, Uruguay 2009 al 2014 – Publicación semanal sobre psicología

obtener información confidencial o para convencerlos de realizar algún tipo de acción que comprometa la integridad de su sistema[40].

A nivel informático se dice que el primer ataque de la historia se produjo un viernes 13 de 1989. “Una revista especializada regalaba disquetes promocionales los cuales resultaron infectados por un virus que afectó decenas de empresas y particulares”[41]. En el mismo momento, “nace el virus Dark Avenger que causa un daño lento en el sistema operativo y en ese mismo año IBM comercializa el primer programa antivirus”[42] esto puso en perspectiva una nueva forma de ver lo que prometía generar grandes ganancias en la protección de la información.

Sin embargo, para 1981 Kevin Mitnick con dos amigos consiguieron colocar en las oficinas de COSMOS (Computer System for Mainframe Operations) de Pacific Bell y obtuvieron el listado de claves de seguridad además combinaciones de las puertas de acceso de varias sucursales; la información que se valoró en 200 mil dólares de la época y luego de ser delatados por la novia de uno de sus amigos les costó su primera condena por un tribunal de menores[43].

5.2.2 La ingeniería social en Colombia.

5.2.2.1 ¿Qué conoce Colombia sobre la ingeniería social? Actualmente se habla muy poco de ingeniería social en Colombia y realmente muy pocas personas conocen el término; sin embargo, es visible un intento por dar conocimiento de la misma a través de algunos medios de comunicación como periódicos, radio y televisión, algunos ejemplos son noticias como: "ingeniería social: El Hackeo Silencioso" de la revista Enter.co donde definen esta como “una técnica de hackeo utilizada para sustraer información a otras personas teniendo como base la interacción social, de tal manera que la persona vulnerada no se da cuenta cómo o cuándo dio todos los datos necesarios para terminar siendo la víctima de un ataque informático. En esta práctica se recurre principalmente, a la manipulación

[40] Pontiroli Santiago, Kasperski, Ingeniería social: Hackeando el sistema operativo del ser humano, actualizado el 23 de diciembre de 2013. Disponible en: https://blog.kaspersky.com.mx/ingenieria-social-hackeando-el-sistema-operativo-del-ser-humano/1839/, Consultado el sábado 06 de mayo de 2017.

[41] RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. “Ingeniería Social, una amenaza informática”, septiembre 2009. Disponible en: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica, Consultado el domingo 07 de mayo de 2017.

[42] FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI, junio 2002. Disponible en: http://www.redalyc.org/pdf/160/16007810.pdf ISSN 1390-1079. Consultado el Domingo 07 de mayo de 2017

[43] Hipertextual.com, JJ Velasco “Kevin Mitnick, un hacker de leyenda en la Campus Party de Valencia”, 14 julio 2011, Disponible en: https://hipertextual.com/2011/07/kevin-mitnick-un-hacker-arrepentido, Consultado el miércoles 25 de mayo de 2017

de la psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que en la cadena de seguridad de la información, el ser humano es el eslabón más débil"[44].

"Ingeniería social, la razón del éxito de los ladrones digitales" del periódico el Tiempo en donde se hace referencia a "el punto más débil de una muralla, bien sea de piedra o cibernética, pueden ser las personas. 'Los cibercriminales sacan provecho de varias premisas sociales: todos queremos ayudar; el primer movimiento es siempre de confianza hacia el otro; no nos gusta decir no, y a todos nos gusta que nos alaben', afirma el experto en seguridad informática de ESET, Pablo Ramos"[45].

5.2.2.2 Casos conocidos donde se ha aplicado técnicas de ingeniería social. Algunos ejemplos conocidos en los que se han realizado ataques de seguridad informática en donde posiblemente se usó ingeniería social.

5.2.2.2.1 Ejemplo 1. "Estudiantes 'hackean' calificaciones de su universidad". "El hecho ocurrió a finales de diciembre pasado en Neiva, capital del Huila (sur), donde los 'hackers', tres estudiantes de ingeniería civil, dos de ingeniería electrónica y uno de ingeniería agrícola, menores de 25 años, accedieron a los sistemas de la Universidad Sur Colombiana, declaró el rector, Hernando Ramírez"[46].

Este caso se presentó en el año 2008 en la Universidad Sur Colombiana "USCO", universidad de gran reconocimiento en la región sur de Colombia; donde estudiantes consiguieron acceder a los sistemas de información de notas de dicha universidad y en donde el centro de tecnología informática detecto "en revisiones de rutina por lo menos ocho fraudes en los que calificaciones como 0 o 1 sobre 5 puntos fueron cambiadas por 4 y 5 con lo cual los alumnos aprobaron varias asignaturas" dichos cambios según indican fueron realizados el 22 y el 31 de diciembre del mismo año donde encontraron 366 notas modificadas y a su vez los atacantes aprovecharon el período de vacaciones; curiosamente todo fue ejecutado desde un café internet lo cual da a entender que dichos atacantes

[44] Hipertextual.com, JJ Velasco "Kevin Mitnick, un hacker de leyenda en la Campus Party de Valencia", 14 julio 2011, Disponible en: https://hipertextual.com/2011/07/kevin-mitnick-un-hacker-arrepentido, Consultado el miércoles 25 de mayo de 2017

[45] MEDINA, Edgar. Redacción Tecnosfera. Ingeniería social, la razón del éxito de los ladrones digitales, El Tiempo, Bogotá, 1 de julio de 2015. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/de-que-se-trata-la-ingenieria-social/16020156, Consulta: lunes, 01 de agosto de 2016.

[46] INFORMADOR.MX. "Estudiantes "hackean" calificaciones de su Universidad", febrero 2009. Disponible en: http://www.informador.com.mx/internacional/2009/75916/6/estudiantes-hackean-calificaciones-de-su-universidad.htm, consultado el 07e Mayo d e2017

contaban con la información necesaria para poder acceder al sistema de información de notas.

5.2.2.2.2 Ejemplo 2. "Cae red de hackers que robó más de $1.000 millones". El día lunes 10 de junio de 2013 fue capturada una red de hackers en la ciudad de Bucaramanga un grupo conformado por dos hombres y tres mujeres quienes obtuvieron ilegalmente 1000 millones de pesos de entidades bancarias. "Según información de la policía, los sujetos hacían transferencias de cuentas y luego retiraban el dinero"[47].

5.2.2.2.3 Ejemplo 3. "Capturan a 22 'mercenarios' informáticos por millonario robo a Colpensiones". En abril 25 del 2014 durante el uso del sistema de pago de nómina de personal público de la administradora colombiana de pensiones se generó una alerta de una situación atípica en una cuenta de ahorros lo cual llego a la realización de una investigación en donde encontraron irregularidades en varias cuentas las cuales luego de la investigación encontraron que recibían dineros por medios no legales; según indica la nota fueron capturados 22 mercenarios grupo compuesto de hackers (quienes rompían las contraseñas), reclutadores y captadores (se encargan de obtener los datos de los titulares y de las cuentas para las transferencias); estos delincuentes informáticos consiguieron capturan un monto de 627 millones de pesos. Según es informado en la noticia por la policía "la modalidad empleada por esta organización criminal consistía en contactar a funcionarios en cuya responsabilidad recaen las áreas de tesorería, sistemas y/o talento humano, donde era instalado un software que facilitaba el acceso a archivos con información financiera para posteriormente realizar las transferencias no autorizadas"[48].

5.2.2.2.4 Ejemplo 4. Publicación del espectador "hackean cuentas de correo de candidatos a rectoría de la universidad nacional". En marzo de 2015 fueron “hackeadas” las cuentas de correo electrónico de los candidatos a la rectoría de la Universidad Nacional de Colombia desde las se enviaron mensajes con información subida de tono a los estudiantes; según informa el espectador uno de estos mensajes contenía lo siguiente: “Deseo invitarlos formalmente a participar esta tarde para emborracharnos con mujerzuelas, juegos de azar; a ver mi página

[47] EL ESPECTADOR. “Capturan a 22 'mercenarios' informáticos por millonario robo a Colpensiones"”, 10 de junio 2013, disponible en: http://www.elespectador.com/noticias/nacional/cae-red-de-hackers-robo-mas-de-1000-millones-articulo-426933, consultado el 10 de Mayo de 2017.

[48] EL ESPECTADOR. “Capturan a 22 'mercenarios' informáticos por millonario robo a Colpensiones"”, 23 de octubre de 2015, disponible en: http://www.elespectador.com/noticias/judicial/capturan-22-mercenarios-informaticos-millonario-robo-co-articulo-594594, consultado el 10 de mayo de 2017.

web donde no hay porno, pero si podrán disfrutar de mis videos"[49]. En parte esto evidencia que la ciberdelincuencia es una problemática más en Colombia.

5.2.2.2.5 Ejemplo 5. Publicación HSB noticias: "Bancolombia advirtió por estafa en red usando la marca del banco". En mayo de 2017 fue lanzada una advertencia por la entidad bancaria Bancolombia en la que se advierte de ataques de ingeniería social mediante la técnica de phishing "La modalidad funciona con un correo de 'cuenta bloqueada' que llega desde el correo informacion@bancolombia.com.co que a su vez enlaza a una cuenta falsa encargada de recoger los datos privados del usuario como las contraseñas y números de autorización"[50].

La advertencia fue publicada por diferentes sitios web con el fin de mitigar el riesgo del ataque, entre los destacados esta la revista Enter.co con su artículo: usuarios Bancolombia: tips para no caer en el ataque de phishing"[51] y Pulzo.com con "Alerta de seguridad informática en Bancolombia ya fue solucionada"[52].

5.2.3 La ingeniería social en mundo. De igual manera como se puede evidenciar en Colombia delitos informáticos que llevaron de la mano técnicas de ingeniería social al igual que otros métodos informáticos; dichos delitos no son la excepción en otros países del mundo sin retornar a la historia de este arte o ciencia como es llamado en algunos casos, es posible visualizar algunos casos puntuales con el fin de mostrar que no hay excepción al momento de un atacante o delincuente informático hacerse de información y obtener un beneficio de ella:

5.2.3.1 Ejemplo 1. "Hackean página web de la universidad católica con sitios pornográficos". En Chile según es informado por el diario La Tercera, piratas informáticos lograron "hackear" el sitio web de la Pontifica Universidad Católica de Chile, "se transformó...en una nueva víctima de los ataques informáticos, puesto...su página web sufrió el hackeo del código fuente de su portada, en la cual se pudo ver por un largo rato varios enlaces a sitios de pornografía. Aunque el

[49] EL ESPECTADOR. "Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional", 17 Mar 2015, disponible en: http://www.elespectador.com/noticias/educacion/hackean-cuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936, consultado el 09 de mayo de 2017

[50] HSB Noticias.com, "Bancolombia advirtió por estafa en red usando la marca del banco ", jueves, 16 de marzo de 2017, disponible en: http://hsbnoticias.com/noticias/tus-finanzas/bancolombia-advirtio-por-estafa-en-red-usando-la-marca-del-b-284930, consultado el 17 de mayo de 2017.

[51] Enter.co, "Bancolombia advirtió por estafa en red usando la marca del banco ", 14 de marzo de 2017, disponible en: http://www.enter.co/chips-bits/seguridad/usuarios-bancolombia-tips-para-no-caer-en-el-ataque-de-phishing/, consultado el 17 de mayo de 2017.

[52] Pulzo.com, "Alerta de seguridad informática en Bancolombia ya fue solucionada", 14 de marzo de 2017, disponible, en: http://www.pulzo.com/tecnologia/respuesta-bancolombia-campana-phishing/PP228776 , consultado el 17 de mayo de 2017.

ataque era prácticamente imperceptible a la vista, pues los enlaces estaban ofrecidos a través de una fuente pequeña y en un lugar no muy visible, las redes sociales fueron las encargadas de difundirlo"[53].

5.2.3.2 Ejemplo 2. "Hackers filtran datos de Harvard, Stanford y Princeton". En octubre del 2012, tan solo un par de meses después, Secure publica un artículo, que más de 50 universidades de los EE.UU fueron víctimas de un grupo de "hackers" llamado Ghost Shell, los cuales filtraron información como "nombre, correo electrónico, contraseña, dirección postal y teléfono de más de 120.000 estudiantes y miembros administrativos de las instituciones educativas"[54] entre ellas: Harvard y Princeton.

5.2.3.3 Ejemplo 3. "Ciberataques a celulares se disparan, según estudio". Los teléfonos inteligentes con sistemas Android son uno de los focos principales de atacantes en el mundo actualmente; a pesar de que el artículo hace mención a ello en el 2013 actualmente sigue sucediendo como lo indica "un tipo de ataques consiste en mensajes comerciales enviados para proponer un falso servicio, contra un módico pago de 10 o 50 céntimos, por ejemplo: generalmente los usuarios no notan el ataque, que se refleja en algunos céntimos de más en sus facturas"[55].

5.2.3.4 Ejemplo 4. "El 50% de las empresas son víctimas de la ingeniería social". La encuesta fue realizada en julio y agosto de 2011 por una empresa de soluciones en seguridad en donde se identificó que alrededor del 48% de empresas encuestadas indican que han sido víctimas de ataques de ingeniería social y en las cuales se encuestaron en Estados Unidos, Canadá, Reino unido, Alemania, Australia y Nueva Zelanda a más de 850 profesionales de seguridad e informática; a su vez esta establece que los costos asociados a cada ataque oscilan entre los U$25.000 a U$100.000 dólares según las personas encuestadas, además costos asociados a gastos de los clientes, pérdida de ingresos, interrupción de la actividad de las empresas y el deterioro de la imagen de la misma. Algunos resultados adicionales encontrados en dicha encuesta son:

[53] LA TERCERA. "Hackean página web de la Universidad Católica con sitios pornográficos", marzo 2012. Disponible en: http://www.latercera.com/noticia/hackean-pagina-web-de-la-universidad-catolica-con-sitios-pornograficos/, consultado el 10 de mayo de 2017

[54] B: SECURE. "Hackers filtran datos de Harvard, Stanford y Princeton", octubre 2012. Disponible en: http://www.bsecure.com.mx/featured/hackers-filtran-datos-de-harvard-stanford-y-princeton, consultado el 10 de mayo de 2017.

[55] EL ESPECTADOR. "Ciberataques a celulares se disparan, según estudio", 26 de junio de 2013, disponible en: http://www.elespectador.com/tecnologia/ciberataques-celulares-se-disparan-segun-estudio-articulo-430140, consultado el 10 de mayo de 2017.

- Los correos electrónicos de phishing que buscan engañar y obtener la confianza del destinatario representan la fuente más común de las técnicas de ingeniería social (47%), seguidos de la información obtenida a través de las redes sociales que contienen fuga de información personal y profesional (39%) y los terminales móviles mal asegurados (12%).
- El afán de lucro es la razón más frecuente de los ataques de ingeniería social seguida del deseo a acceder a información confidencial de la empresa (46%), la búsqueda de ventajas competitivas (40%) y los actos de venganza (14%).
- Los nuevos trabajadores o colaboradores son los más vulnerables a las técnicas de ingeniería social.
- El 34% de las empresas no han capacitado a los trabajadores en políticas de seguridad para evitar caer en los ataques de ingeniería social.[56]

5.2.3.5 Ejemplo 5. “¡no tan rápido! esa publicación de Facebook podría no ser lo que parece”. Sitios web patrocinados por algunas empresas de seguridad también buscan mantener informados a los usuarios con artículos de interés como "¡No tan rápido! esa publicación de Facebook podría no ser lo que parece"[57] en donde se habla de amenazas comunes en la red social de Facebook mediante publicaciones falsas, perfiles sociales falsos y demás explicando cómo funciona este ataque de ingeniería social mediante publicaciones en redes sociales y que hacen los delincuentes informáticos con la información que consiguen.

5.3. MARCO CONCEPTUAL

En la actualidad las personas encuentran un mundo interconectado debido a diferentes necesidades de información y gracias a la red de internet con la cual es posible acortar distancias y conseguir de una manera más sencilla información además de permitir ponerse en contacto con gente de diferentes lugares; también existe la tendencia de las personas a confiar en lo que se encuentra a su alrededor motivo por el cual los delincuentes han encontrado un campo de acción en donde pueden permanecer en el anonimato contando con una mínima exposición a ser descubiertos y capturados consiguiendo generar grandes oportunidades de lucro mediante el cibercrimen dentro de las modalidades de técnicas para este se encuentra la ingeniería social en la cual se centra este proyecto; en cuanto al termino este se remonta a las ciencias políticas en donde

[56] es.ccm.net "El 50% de las empresas víctimas de la ingeniería social", actualizado en mayo 2017, disponible en: http://es.ccm.net/faq/7695-el-50-de-las-empresas-victimas-de-la-ingenieria-social, consultado el 17 de mayo de 2017.

[57] WeLiveSecurity.com, Noticias, opiniones y análisis de la comunidad de seguridad de ESET, "¡No tan rápido! Esa publicación de Facebook podría no ser lo que parece ", publicado en febrero 3 de 2016, disponible, en: https://www.welivesecurity.com/la-es/2016/02/03/no-tan-rapido-publicacion-de-facebook/ , consultado el 17 de mayo de 2017.

hacen referencia a influir actitudes, cambiar comportamientos, manipular individuos o grupos sociales.

Con el cambio constante y rápido de las tecnologías de información los delitos evolucionan y la mayoría de las personas desconocen que es la ingeniería social, motivo que los lleva a menudo a ser víctimas de delincuentes que aprovechan la ignorancia sobre el tema y logran sustraer información o dinero gracias a técnicas como phishing, baiting, duster diving o cualquier otra técnica asociada que se ajuste a la víctima; los inicios se enfocan en la informática y como la conocemos en la actualidad se remontan a Kevin Mitnick quien propone que todo ingeniero social se basa en los siguientes 4 principios del ser humano: [21].

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir no.
- A todos nos gusta que nos alaben.

Como lo menciona Pablo M. Caruana, la ingeniería social "básicamente se denomina como todo artilugio, tretas y técnicas más elaboradas a través del engaño de las personas en revelar contraseñas u otra información, más que la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema"[58].

Entendiendo el alcance de la ingeniería social es evidente la importancia de dar a conocer, informar y capacitar a las personas en las diferentes técnicas que existen para este tipo de ataques con la finalidad de contar con el conocimiento necesario para poder perspicazmente reconocer y contrarrestar cualquier ataque del cual puedan estar siendo o sean víctimas.

En la actualidad Promociones y Cobranzas Beta no cuenta con una forma de mitigar riesgos frente a ataques de ingeniería social de los cuales pueden ser víctimas, motivo por el cual este proyecto es de crucial importancia para la empresa.

5.3.1 Promociones y Cobranzas Beta. Es una Institución de cobranzas líder en servicio, innovación, agilidad y eficacia, soportada por un personal con cultura de calidad, óptimamente preparado y con gran vocación de servicio.

[21] K. Mitnick and W. Simon, The art of deception. Indianapolis: Wiley, 2002.

[58] Caruana, Pablo M, "Breves Conceptos sobre la Ingeniería Social", 2001, disponible en http://virusattack.xnetwork.com.ar/articulos/VerArticulo.php3?idarticulo=4 , consultado el Domingo, 02 de octubre de 2016.

Fue fundada en 1986, contando en la actualidad con 30 años de experiencia en la actividad de cobranzas y presencia en 18 ciudades del país.

Actualmente, la actividad de cobranza está dirigida de manera exclusiva a la cartera del Banco Davivienda.

Es una entidad vigilada por la Superintendencia de Sociedades y hace parte del grupo empresarial liderado por Sociedades Bolívar S.A.; en desarrollo de su objeto social, recolecta y administra información de direcciones, teléfonos y correos electrónicos; datos necesarios y fundamentales para mantener informados a los clientes del Banco Davivienda y de Cobranzas Beta sobre el estado actual de sus obligaciones y sobre alternativas de pago y beneficios adicionales que le permitan al cliente mantener al día sus productos o lograr mejorar sus reportes de comportamiento en el sector financiero; igualmente recolecta y administra información adicional que en un momento dado es requerida por el Banco Davivienda y por Cobranzas Beta para que el cliente pueda recibir los beneficios adicionales que se le ofrecen, los cuales corresponden principalmente a descuentos en saldos de capital, descuentos en saldos de intereses, descuentos en saldos de otros conceptos o disminuciones de tasas de interés[59].

5.3.2 Geográficamente. Promociones y Cobranzas Beta cuenta con 18 sucursales a nivel nacional divididas en clase A, B y C dependiendo de su tamaño respecto al número de trabajadores con los que cuenta la sucursal, dentro de la cuales encontramos a: Bogotá, Armenia, Barranquilla, Bucaramanga, Cali, Cartagena, Cúcuta, Ibagué, Manizales, Medellín, Montería, Neiva, Pasto, Pereira, Santa Marta, Tunja, Valledupar y Villavicencio.

Su personal de planta tiene a disposición a 750 empleados de los cuales el 80% son asesores de cobranzas quienes están en constante contacto con personal externo como usuarios y clientes internos de la empresa a quien brindan los servicios; el restante 20% corresponde a las áreas administrativas, las cuales están conformadas por el área contable, sistemas, administrativa, RRHH y operaciones, quienes mantienen un contacto frecuente con el cliente interno, proveedores y outsourcing.

De estas personas se busca que 463 sean informadas mediante el plan de concientización sobre la exposición a ataques de ingeniería social a la que se encuentran expuestos en la empresa y serán quienes estarán involucrados con el plan.

[59] Promociones y Cobranzas Beta, "Nuestra Empresa", no disponible fecha de publicación, disponible en: http://cobranzasbeta.com.co/desarrollo/content/nuestra-empresa, consultado el 28 de junio de 2017

5.3.3 Objetivo organizacional de promociones y cobranzas beta. En la Ilustración 2. Objetivo organizacional, se puede ver el objetivo organizacional de la empresa.

Ilustración 2. Objetivo organizacional

Fuente: Promociones y Cobranzas Beta, disponible en http://cobranzasbeta.com.co/desarrollo/content/nuestra-empresa

5.3.4 Líneas de negocio de promociones y cobranzas beta. En la Ilustración 3. Líneas de negocio, se mencionan las líneas de negocio que trabaja la compañía.

Ilustración 3. Líneas de negocio

Fuente: Promociones y Cobranzas Beta, disponible en: http://cobranzasbeta.com.co/desarrollo/content/nuestra-empresa,

5.4. MARCO LEGAL

El marco legal de la seguridad informática en Colombia es muy importante ya que gracias a este se regula, decreta e indica la normatividad que se debe cumplir, actualmente a nivel nacional en Colombia para delitos informáticos rigen las siguientes leyes en lo que se refiere a seguridad informática y pueden ser tenidas en cuenta para la ingeniería social:

5.4.1 Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual "dicta disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".[60]

Por disposición de la ley la información almacenada en bancos de datos y archivos de entidades privadas y públicas solamente puede ser interceptada o registrada mediante orden judicial según los casos y mediante la forma que la ley lo

[60] Colombia. Congreso de la república. LEY ESTATUTARIA 1266 DE 2008: "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". Bogotá, D. C., a 31 de diciembre de 2008.

establezca; por lo cual al presentarse un ataque de ingeniería social se estaría accediendo ilegalmente o sin el consentimiento del propietario a información almacenada en bases de datos o archivos con información personal de usuarios.

5.4.2 Ley 1273 del 5 de enero de 2009 Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

Esta ley se divide en dos capítulos: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero hace referencia a los siguientes artículos.

5.4.2.1 Artículo 269a. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.4.2.2 Artículo 269b. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legal es mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

5.4.2.3 Artículo 269c. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

5.4.2.4 Artículo 269d. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.4.2.5 Artículo 269e. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.4.2.6 Artículo 269f. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.4.2.7 Artículo 269g. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

5.4.2.8 Artículo 269i. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239, manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

5.4.2.9 Artículo 269j. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes[61].

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Por medio de la 1273 de 2009 se busca proteger a los civiles, empresas privadas y empresas públicas de ataques Informáticos independientemente de la técnica que sea usada; los artículos anteriormente mencionados cubren los alcances de las mismas, por ejemplo: si es realizado un ataque de phishing se estaría infringiendo varios de los artículos de esta ley; al igual que si se usa cualquier de las técnicas de ingeniería social.

5.4.3 Ley estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”[62]. Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma por disposición de la ley la información almacenada en bancos de datos y archivos de entidades privadas y públicas solamente pueden ser interceptada o registrada mediante orden judicial según los casos y mediante la forma que la ley lo establezca; al presentarse un ataque de ingeniería social se estaría accediendo ilegalmente a información almacenada en bases de datos o archivos (Impresos o digitales) con información personal de usuarios; esta ley busca proteger el tratamiento de los datos en el ámbito personal o doméstico motivo por el que al presentarse un ataque de esta

[61] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4

[62] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan Disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1

índole en la cual se acceda a datos personales estos se estarían accediendo sin autorización del titular o dueño de los datos infringiendo la ley 1581 de 2012.

5.4.4 Ley 23 de 1982 sobre derechos de autor “Sobre derechos de autor.”[63] Esta ley tiene como finalidad proteger los derechos de autor, es decir que toda obra creada por el ingenio humano en cualquier campo (científico, artístico y literario por nombrar algunos) quedará salvaguardado y se garantizaran los derechos patrimoniales y morales.

La ley hace referencia a como el autor puede reclamar los derechos sobre su obra oponerse a transformaciones, publicaciones sin autorización y otras acciones que puedan afectar los derechos morales de la obra los cuales son intransferibles e imprescriptibles.

Así mismo la ley hace énfasis en derechos patrimoniales los cuales permiten al autor explotar su obra en forma económica por medio de los derechos podrá autorizar su comercialización, autorizar transformaciones y difusiones entre otros derechos ganados; el término de duración se limita a la vida del autor más 80 años después de su deceso.

De esta manera quien utilice, copie o transforme una obra creada por el ingenio humano en la Republica Colombiana estará violando la ley; al momento de realizar la técnica de phishing se está plagiando la identidad de páginas web; al realizar la técnica Vishing se está clonando un IVR telefónico; al realizar la técnica baiting se está utilizando sin autorización logos y nombres de entidades con derechos de autor.

[63] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 23. (28, enero, 1982). “Sobre derechos de autor”. Bogotá, D.C., a 28 de enero de 1982.

6. METODOLOGÍA

Según los objetivos y alcances definidos para este proyecto, se abordará el tipo de investigación descriptivo siguiendo una serie de pasos que buscan identificar y definir factores, elementos, características y procedimientos con la finalidad de concientizar al personal de Promociones y Cobranzas Beta frente a la amenaza de la ingeniería social y como esta afecta a la empresa y a las personas. Así se ubica este proyecto dentro de un contexto para diseñar un plan que entregue a los empleados de la empresa una alternativa de conocimiento para hacer frente a esta amenaza.

Mediante esta investigación se pretende encontrar vulnerabilidades detectadas en el recurso humano de la compañía al igual que de sus respectivas áreas de trabajo, de esta manera hacer frente a posibles ataques de ingeniería social informando al personal de los métodos o técnicas de esta temática usadas por los delincuentes informáticos para conseguir accesos a información que les permita dar de una u otra forma con datos sensibles. De esta manera se da a conocer la necesidad en el personal para identificar posibles maneras de ataque de dicha índole al igual que consecuencias que puede acarrear o traer esta.

Para dar ejecución a este proyecto, se dividió en las siguientes fases o etapas:

- Fase 1: Reconocimiento, recolección, y análisis de información sobre el estado Inicial, antes de ejecutar plan de concientización.
- Fase 2: Ejecución de plan de concientización.
- Fase 3: Análisis del estado luego de ejecutar el plan de concientización.

Las fases fueron expuestas y aprobadas por Promociones y Cobranzas Beta S.A., Anexo A. Acta de reunión 1, y serán abordadas en detalle a continuación de este documento.

Una vez finalizado este proyecto la información de la metodología podrá ser aplicada a otras organizaciones ya que este busca informar y crear conciencia sobre como delincuentes usan técnicas de ingeniería social para obtener información importante de una empresa de forma sutil, sencilla y en muchos casos sin dejar rastro.

A continuación, se muestra la puesta en marcha y ejecución de este.

7. FASE 1 - RECONOCIMIENTO, RECOLECCIÓN, Y ANÁLISIS DE INFORMACIÓN

Busca identificar y recolectar la mayor cantidad de información posible sobre el conocimiento que tiene el personal de Promociones y Cobranzas Beta sobre la ingeniería social.

7.1 POBLACIÓN

Como población se busca informar y concientizar a 463 empleados de la empresa Promociones y Cobranzas Beta, los cuales debido a sus funciones y roles de acceso a diferentes tipos de información sensible y equipos de cómputo podrían ser víctimas de ataques informáticos.

Población empleados por sede Promociones y Cobranzas Beta:

- Bogotá: 213 Personas.
- Regional Armenia: 8 Personas.
- Regional Barranquilla: 23 Personas.
- Regional Bucaramanga: 16 Personas.
- Regional Cali: 31 Personas.
- Regional Cartagena: 18 Personas.
- Regional Cúcuta: 14 Personas.
- Regional Ibagué: 14 Personas.
- Regional Manizales: 10 Personas.
- Regional Medellín: 39 Personas.
- Regional Montería: 8 Personas.
- Regional Neiva: 10 Personas.
- Regional Pasto: 6 Personas.
- Regional Pereira: 10 Personas.
- Regional Santa Marta: 10 Personas.
- Regional Tunja: 10 Personas.
- Regional Valledupar: 10 Personas.
- Regional Villavicencio: 13 Personas.

7.2 RECOLECCIÓN DE INFORMACIÓN Y FUENTES

La información recolectada de la empresa Promociones y Cobranzas Beta se recolecto de la siguiente manera:

7.2.1 Información entregada por la empresa. Gracias al apoyo de la compañía fue posible contar con información como: Listado de directorio telefónico interno,

donde se pueden apreciar extensiones asignadas, correos electrónicos, nombres completos, cargos, áreas y sedes.

- El recurso interno informa de: horarios de funcionamiento de las oficinas, labor desempeñada por empleados y áreas, aspectos puntuales sobre información de empleados como por ejemplo aquellos que se levantan del puesto sin bloquear el equipo o quienes manejan papelería en la empresa, además de sitios frecuentados por los colaboradores para salir a almorzar.
- Uso de servicios telefónicos y de red, además de acceso a internet y uso de medios de almacenamiento externos.
- En el Anexo A. Acta de reunión 1, se indican los documentos entregados y usados para la ejecución de este proyecto.

7.2.2 Información encuesta. La encuesta se realiza mediante muestreo aleatorio simple en el cual se concretó un tamaño de la muestra mínima y se extrajeron al azar los elementos[64]; con la muestra se identifica si trabajadores cuentan con algún conocimiento acerca de la ingeniería social.

Para la encuesta realizada en la etapa 1 participaron 98 personas quienes eligieron llenar la encuesta por voluntad propia; este grupo representa el 21% de la población; se presentó una gran abstención en la participación debido a que en su mayoría no están relacionadas con el término y la temática.

El tamaño de la muestra se realizó usando la fórmula para población finita de Murray y Larry (2005), la cual se enseña en la Ilustración 4. Fórmula muestreo.

Ilustración 4. Fórmula muestreo

$$n = \frac{Z_{\alpha}^{2} \cdot N \cdot p \cdot q}{i^{2}(N-1) + Z_{\alpha}^{2} \cdot p \cdot q}$$

Fuente: Estadística. Serie Schaum- 4ta edición - Murray R. Spiegel (2009)

Para la muestra con la encuesta voluntaria se busca que por lo menos 80 personas respondan la misma para contar con un muestreo inicial con un 10% de error como máximo para identificar que tanto se conoce sobre el tema al interior de la empresa y contando con un margen de confiabilidad de la misma de un 95%;

[64] Dr. Rodriguez, Ernesto, "Tema: Muestra y Muestreo", 2012, disponible en https://www.uaeh.edu.mx/docencia/P_Presentaciones/tizayuca/gestion_tecnologica/muestraMuestreo.pdf, consultado el jueves, 13 de Julio de 2017.

adicionalmente se realizan unas pruebas de ataques de ingeniería social buscando enfocar el plan de concientización, las cuales son apoyadas por Promociones y Cobranzas Beta quien entrega para esta información detallada …en el parágrafo 7.2.1… permitiendo establecer objetivos puntuales para realizar las mismas tomando mínimo una persona de cada área como posible víctima de al menos una prueba de ataque de dicha índole.

En el parágrafo 7.1… se detallan las sedes y cantidad de personas en cada una de ellas en las cuales se encuentran distribuidas los 463 empleados de donde se obtiene la muestra para los resultados de la encuesta.

Aunque no se alcanzó el 100% del personal de Promociones y Cobranzas Beta los cuales suman 463 empleados en 17 regionales del país con la sede principal ubicada en Bogotá, la muestra recolectada permite evidenciar la necesidad de capacitar al personal sobre los riesgos que representa la ingeniería social para la empresa, las personas y sus familias.

En el parágrafo 7.6 y 7.7, se encuentra la encuesta realizada y análisis de la misma para la fase 1;…en el parágrafo 6.1 y 6.2 se puede observar la encuesta y análisis realizados de la fase 3.

7.2.3 Información identificada mediante observación. Mediante la observación se identificó nueva información y se confirmó alguna otra como:

- Tiempos de actividades de empleados, y horarios laborales.
- Tiempos de inactividad de equipos.
- Manejo de papelería.
- Formas de acceso físico a la empresa.
- Practicas no recomendadas con papelería, al igual que de uso de computadores.
- Actividades diarias realizadas, y publicaciones visibles desde sitios de atención.
- Disposición del personal, en cuanto a la ayuda y atención a los usuarios.
- Organización de documentos físicos puntualmente cerca de impresoras, puestos y mesas de trabajo.

7.2.4 Información del acuerdo de confidencialidad. Según lo acordado con Promociones y Cobranzas Beta en el acuerdo de confidencialidad firmado por el representante legal y por las partes ejecutoras de este proyecto, la información mencionada como confidencial dentro del mismo podrá ser tenida en cuenta como muestra para fines informativos, pero no será entregada en su totalidad con datos

que puedan comprometer la integridad de información sensible de la empresa o derechos de autor de la misma.

En el Anexo D. Acuerdo de confidencialidad, se encuentra una copia del documento firmado por ambas partes.

7.2.5 Get-out-of-jail (salida de la jaula). Para efectos prácticos en caso de presencia legal, judicial y/o procesal, de un delito informático informado por un funcionario no autorizado de la compañía en pro de este y con el fin de actuar frente a posibles delitos detectados antes de que sean ejecutados y a su vez este actué llamando a seguridad o a las autoridades competentes por parte de la empresa Promociones y Cobranzas Beta, se entrega una carta de get-out-of-jail en donde el director del área de sistemas de la empresa, quien es el responsable del proyecto autoriza explícitamente a los ejecutores de este proyecto para realizar las pruebas de ingeniería social descritas y ejecutadas con este; una copia del documento se encuentra en el Anexo E. Get out of jail.

7.3 EJECUCIÓN PRUEBAS DE INGENIERÍA SOCIAL - FASE 1

Contando la información inicial entregada por la compañía se realiza un análisis de los posibles escenarios donde los trabajadores de Promociones y Cobranzas Beta pudiesen ser vulnerables a ataques de ingeniería social; en esta fase se recolecta información referente a la constitución de la empresa, organigrama, presencia en redes sociales, números de teléfonos y directorios telefónicos, para perfilar y analizar a los empleados de la empresa y los procesos que realizan. En el Anexo A. Acta de reunión 1, se detallan los documentos entregados por la entidad; en el Anexo F. Documentos entregados por Promociones y Cobranzas Beta, se muestra el contenido de la documentación.

Contando con la información provista por la firma se realizó un documento en donde se especifican las pruebas de ingeniería social a realizar y a cuáles personas o cargos de la empresa se realizarán; estas son aprobadas y autorizadas por el director de sistemas; en el Anexo B. Acta de reunión 2;…Véase en el numeral 7.4, detalle de las pruebas a realizar a la compañía.

Las pruebas de ingeniería social planteadas se enfocan en la selección de ataques específicos en la empresa, además de direccionar los mismos dentro de una selección de objetivos (personas) en la compañía, los cuales son susceptibles a ser posibles víctimas de los diferentes tipos de ataques de esta índole según el rol y características de funciones desempeñadas; para ello son usados los siguientes tipos de ataques:

- Phising.

- Baiting.
- Pretexting.
- Dumpster diving.
- Shoulder surfing.
- Ingeniería social en las redes sociales.

7.4 PRUEBAS DE INGENIERÍA SOCIAL FASE 1 A PROMOCIONES Y COBRANZAS BETA

La siguiente lista contiene los objetivos seleccionados de acuerdo a características específicas que los hacen más vulnerables o más atractivos de acuerdo a la información que manejen, el cargo que desempeñen dentro de la compañía, o el objetivo de información de un posible atacante.

7.4.1 Phishing

7.4.1.1 Vulnerabilidad. Usuarios que confían en correos publicitarios, de dudosa procedencia.

7.4.1.2 Objetivo. Obtener datos enviando información falsa; se busca que el usuario de clic en un link enviado por correo electrónico el cual contiene publicidad de una reconocida empresa que entrega beneficios para Promociones y Cobranzas Beta S.A y quien a su vez es la caja de compensación familiar que tiene la empresa; este tipo de correos es muy común que sean recibidos por los empleados de la compañía de forma masiva al email corporativo por lo cual se espera que las personas sean víctimas de un ataque controlado al dar clic sobre la imagen de la publicidad, la cual enviara la información básica del usuario como lo es: dirección IP del equipo desde donde se dio clic en la red interna, hora de la consulta y desplegara un formulario el cual se ejecuta en un servidor web local con una IP interna expuesta, la cual solicitara el registro con el usuario de correo, nombre y apellido; dicho correo realizado para el ataque controlado se envía a la lista general de la compañía desde una cuenta creada en Gmail con el nombre info**.**nombreempresacajadecompensacionfamiliar@gmail.com, con esta prueba se espera que el 10% de las personas den clic sobre las imágenes de la publicidad y que el 1% ingrese los datos solicitados en el formulario; el número total de los correos a los cuales se les enviara la publicidad falsa es de 463, esto cubre las 18 ciudades en las que tiene presencia la empresa a nivel nacional.

7.4.1.3 Descripción usuarios objetivo. Los objetivos seleccionados son usuarios y áreas que cuentan con privilegios de navegación, recepción y envió de correos,

factores que los hacen más propensos a este tipo de ataques; mediante observación e investigación se encontró que Promociones y Cobranzas Beta en anteriores oportunidades ha tenido recepción de correos con phishing. En el cuadro 1. Objetivos phishing, se menciona el nombre del área a realizar la prueba, el responsable de esta y la cantidad de personas a quienes se enviará el correo

Cuadro 1. Objetivos phishing

Nombre del área	**Responsable**	**Cantidad de personas**
Beta Nacional	Gerente General	463

Fuente: Diseñadores del proyecto.

7.4.2 Baiting.

7.4.2.1 Vulnerabilidad. Confianza en medios de almacenamiento externos (Pen Drives, CD´s, DVD´s) de procedencias desconocidas con los cuales es posible sustraer información, capturar datos del usuario, instalar o propagar virus y ejecutar software para tomar control total de un equipo de cómputo.

7.4.2.2 Objetivo. Sustraer información y ejecutar código o herramientas; al momento de usar el dispositivo de almacenamiento externo se ejecuta automáticamente una aplicación para capturar información como dirección IP, hostname, fecha y hora de ejecución, se evidenciará la falta de medidas de seguridad que se deben tener al conectar unidades a los equipos de compañía; La metodología usada será enviando un cd con un ejecutable que se activa al ingresar el dispositivo al pc, el cd se envía con logotipos de publicidad sobre viajes turísticos a precios muy atractivos, con el fin de incitar a las víctimas a conocer más sobre la información contenida en el medio de almacenamiento; a los usuarios ubicados en la ciudad de Bogotá se les dejaran cd´s con carátulas de música previamente seleccionada de acuerdo a gustos musicales de las víctimas.

7.4.2.3 Descripción usuarios objetivo. Los objetivos seleccionados son usuarios y áreas que cuentan con privilegios para conectar dispositivos, debido a que estos tienen una mayor exposición a este tipo de ataques. En el Cuadro 2. Usuarios objetivos baiting, se detalla el cargo de la persona objetivo y la dirección IP del equipo asignado a este para sus labores diarias en la sede de Bogotá; en Cuadro 3. Áreas objetivas baiting se mencionan las áreas, responsables y cantidad de personas, quienes serán las metas a alcanzar en las sedes anexas.

Cuadro 2. Usuarios objetivos baiting

Cargo	**IP**
Coordinador administrativo	172.10.104.91
Editora de capacitación	172.10.107.77
Jefe de contabilidad	172.10.105.73
Analista de desarrollo	172.10.110.95

Fuente: Diseñadores del proyecto.

Cuadro 3. Áreas objetivas baiting

Nombre del área	**Responsable**	**Cantidad de Personas**
Directores regionales	N/A	18

Fuente: Diseñadores del proyecto.

7.4.3 Pretexting

7.4.3.1 Vulnerabilidad. Usuarios que por su buena fe de ayudar confían en personas externas o ajenas, quienes manipulan mediante una llamada dichas acciones con el fin de obtener información.

7.4.3.2 Objetivo. Obtener información mediante el uso de guiones previamente creados; la metodología es realizar llamadas a los auxiliares operativos de las regionales de Promociones y Cobranzas Beta, ya que estos manejan una gran cantidad de aplicativos con sus usuarios y respectivas claves; para esta prueba se intentará capturar la contraseña del dominio, ya que esta se encuentra atada a varios programas entre ellos el correo electrónico el cual es posible accederlo desde la red externa, se simulará ser una persona nueva en el área de soporte de sistemas, ya que es constante el ingreso y salida de aprendices del Sena, los cuales realizan sus pasantías y duran unos pocos meses antes de ser reemplazados por otros; mediante un guion y con información recopilada previamente se le pedirá la contraseña de correo con el fin de validar un posible virus.

Por otro lado se realizará una prueba al área de sistemas ya que se encontró una debilidad en el procedimiento de desbloqueo de cuentas de dominio y en el flujo de información del área de recurso humanos (RRHH) sobre retiros de personal de la empresa; se simulara ser una persona que recién salió de la empresa según información conseguida en hojas recicladas encontradas en una bandeja de impresión, procediendo a llamar al área de soporte, valiéndose de otra

vulnerabilidad encontrada en la conexión de las troncales telefónicas que conectan a las ciudades las cuales si se realiza una transferencia desde el exterior a extensiones internas no arrojan el identificador de la línea haciendo creer al receptor que la llamada es interna, se pide el cambio de contraseña por bloqueo de la misma esperando que esta sea cambiada sin solicitar ningún soporte.

7.4.3.3 Descripción usuarios objetivo. Los objetivos seleccionados son usuarios y áreas que tienen acceso a llamadas telefónicas desde el exterior y que cuentan con permisos de usuarios en aplicaciones importantes tales como correo, dominio y generador de Tickets GLPI.

- 5 llamadas como externo.
- 5 llamadas como interno.

En el Cuadro 4. Personal objetivo de pretexting se especifica el cargo e IP de los objetivos externos a la sede de Bogotá; en el Cuadro 5. Áreas objetivo de pretexting se menciona el área, responsable e IP para las llamadas de sistemas.

Cuadro 4. Personal objetivo de pretexting

Cargo	**IP**
Auxiliares operativos	172.10.X.102

Fuente: Diseñadores del proyecto.

Cuadro 5. Áreas objetivo de pretexting

Nombre del Área	**Responsable**	**Cantidad de Personas**
Área sistemas	Auxiliar sistemas	172.10.110.X

Fuente: Diseñadores del proyecto.

7.4.4 Dumpster diving

7.4.4.1 Vulnerabilidad. Descuido de documentos con información importante o sensible, hojas en impresoras o botes de basura.

7.4.4.2 Objetivo. Recolectar hojas dejadas en impresoras, lugares de papel reciclable y papeleras de basura; con estos documentos se busca posible información valiosa la cual se analizará y seleccionará según la relevancia para planificar los ataques de ingeniería social a realizar a los objetivos seleccionados.

7.4.4.3 Descripción usuarios objetivo. Los objetivos seleccionados son todas las áreas que cumplen con la vulnerabilidad. En el Cuadro 6. Áreas objetivo dumpster diving se especifica el área responsable y la cantidad de personas afectadas por esta prueba.

Cuadro 6. Áreas objetivo dumpster diving

Nombre del área	Responsable	Cantidad de Personas
Sede Bogotá	N/A	200

Fuente: Diseñadores del proyecto.

7.4.5 Shoulder Surfing.

7.4.5.1 Vulnerabilidad. Por falta de recordación algunos empleados colocan su clave de red escrita en un papel visible o permiten ver su clave de red fácilmente al digitarla, también aplican los usuarios que dejan sin bloquear las pantallas permitiendo ver la información contenida en los aplicativos abiertos.

7.4.5.2 Objetivo. Obtener usuarios y contraseñas de red que permitan tener acceso al perímetro de seguridad; la metodología usada será dar rondas por el edificio en busca de personas que están tecleando usuarios y contraseñas en aplicativos o al ingresar al dominio de red, también se verifican los papeles pegados en los computadores en busca de contraseñas y usuarios.

7.4.5.3 Descripción usuarios objetivo. Los objetivos de este ataque son todas las personas que por descuido dejan sus contraseñas visibles, personas que al digitar información de contraseñas no se cercioren que los estén vigilando. El Cuadro 7. Objetivos shoulder surfing se menciona la sede, cargos, IP, vulnerabilidades y objetivos para la prueba

Cuadro 7. Objetivos shoulder surfing

Nombre	Cargo	IP	Vulnerabilidad	Objetivo
Sede Bogotá	Todos	N/A	Pantallas sin bloqueo, claves predecibles y contraseñas pegadas en el escritorio.	Acceso a equipo sin autorización del funcionario.

Fuente: Diseñadores del proyecto.

7.4.6 Ingeniería social en las redes sociales.

7.4.6.1 Vulnerabilidad. Usuarios quienes, por buena fe o por falta de medidas de control en las redes sociales, permiten que personas que no las conocen tengan acceso a la información publicada en sus perfiles; estas personas aceptan a desconocidos sin indagar si realmente son fiables, sin indagar si los perfiles son verdaderos o falsos, quedando expuestas a compartir información personal con un posible atacante.

7.4.6.2 Objetivo. Poder ver la información que suben los usuarios a la red con el fin de recaudar información personal, la cual permite realizar una perfilación de la víctima para crear una estrategia de ataque; la metodología utilizada será crear un perfil falso de apariencia agradable y confiable; se tomará prestado el perfil de un amigo el cual accedió a prestar el contenido; (fotos, gustos y otra información la cual permitirá dar un aspecto familiar), se enviaran invitaciones de amistad partiendo de dos personas encontradas por la red social Linkedin las cuales tienen perfil de Facebook y que trabajan en Promociones y Cobranzas Beta, a partir de estas dos personas se buscaran lazos de amistad con el resto de la comunidad de Beta, logrando tener más personas en común lo cual provocara que más personas confíen en el perfil falso vinculando a otros perfiles.

7.4.6.3 Descripción usuarios objetivo. Los objetivos son todos aquellos empleados que se encentren con información pública en redes sociales, con cuentas mal parametrizadas y que acepten invitaciones de perfiles desconocidos sin indagar su veracidad, se incluirán solo colaboradores, en el Cuadro 8. Objetivos ingeniería social en redes sociales se referencia la finalidad de la prueba, vulnerabilidad y quienes son objetivos. En la siguiente tabla se referencia las sedes, cargos, IP, vulnerabilidad y objetivos del test.

Cuadro 8. Objetivos ingeniería social en redes sociales

Nombre	**Cargo**	**IP**	**Vulnerabilidad**	**Objetivo**
Nacional	Todos	N/A	Usuarios con perfiles publicados en Facebook u otras redes sociales con vínculos con la empresa.	Ganar confianza víctima y solicitar información.

Fuente: Diseñadores del proyecto.

7.5 ANÁLISIS PRUEBAS DE INGENIERÍA SOCIAL - FASE 1

Luego de realizadas las pruebas en la primera fase de este proyecto, mediante las técnicas de suplantación de identidad, phishing, baiting, pretexting y tailgating se logró quebrantar la seguridad, encontrando diferentes tipos de vulnerabilidades; a continuación, se describirán las vulnerabilidades encontradas y como se deben remediar o mitigar según sea el caso:

7.5.1 Hallazgo sin realizar pruebas troncales plantas telefónicas entre ciudades. Haciendo uso de la observación y con la ayuda del recurso interno en la compañía, se encontró que al momento de transferir las llamadas, el identificador de llamada (caller id) de la línea original se pierde; esto facilita la aplicación de la técnica pretexting y puede ser utilizado para facilitar un ataque; la vulnerabilidad fue explotada al llamar desde un teléfono externo, marcando a una extensión de Promociones Y Cobranzas Beta Bogotá, pidiendo transferir la llamada a una regional, llegando a la extensión remitida de la regional un caller id que usa la troncal interna e identificándose como Bogotá; esta falencia sucede al momento de comunicar los dos servidores Asterisk y es una falla de configuración de los mismos.

7.5.2 Pretexting. Aprovechando la información mencionada …véase en el numeral 5.4.5.1… realización de pruebas con la técnica de pretexting; en la prueba 1 el atacante llama a la recepción en Bogotá o al recurso interno y pide ser remitido a una regional, una vez remitido a la regional se presenta como un auxiliar del SENA que ingresó hace poco a trabajar dentro de la empresa; la llamada tiene como objetivo los auxiliares operativos de las regionales, argumentando la revisión del correo electrónico ya que la consola de antivirus detecta un posible contagio y se necesita realizar una verificación directa sobre la cuenta de correo electrónico, en donde se pide a la víctima el usuario de correo electrónico y red, además de la contraseña; es importante resaltar que las credenciales del correo son las mismas del dominio de red; bajo este argumento varios auxiliares operativos accedieron a entregar la información solicitada sin oponer mucha resistencia.

En la prueba 2 el atacante realiza suplantación de exempleados; mediante el ataque se detecta que la información de salida de personal no se informa con rapidez y efectividad, pues al salir una persona de la empresa pueden pasar más de 5 días antes de que sea retroalimentada el área de sistemas y se proceda a bloquear el usuario.

7.5.2.1 Resultado de la prueba 1. Inicialmente se buscó realizar pruebas de pretexting a diecisiete (17) personas con el cargo de auxiliar operativo en cada

sede; sin embargo, se realizaron once (11) llamadas de las cuales diez (10) fueron efectivas y una (1) no fue posible culminarla; las llamadas se realizaron a los auxiliares operativos de las siguientes ciudades:

- Cúcuta.
- Armenia.
- Montería.
- Pasto.
- Santa Marta.
- Neiva.
- Pereira.
- Manizales.
- Tunja.
- Valledupar.
- Barranquilla.

Las restantes llamadas no se realizaron ya que se presentó una alerta entre los auxiliares gracias a que uno de ellos contactó al área de sistemas e indagó sobre la autenticidad del auxiliar del SENA, quien solicitó usuario y contraseña de su cuenta de correo, el personal de sistemas negó la existencia del falso auxiliar e hizo que todos los auxiliares operativos de las regionales se comunicaran y alertaran sobre las llamadas fraudulentas.

7.5.2.2 Transcripción llamada de ejemplo prueba 1. A continuación, un ejemplo mediante la transcripción de una llamada:

Víctima: "Promociones y Cobranzas Beta buenos días, habla Jeniffer Ortiz en que le puedo colaborar."

Atacante: "hola Jennifer, ¿cómo estás?, hablas con Juan Rodríguez, yo soy el nuevo auxiliar de sistemas del Sena, entré la semana pasada como el viernes."

Víctima: "a bueno."

Atacante:"mira lo que pasa es que se detectó un problema de unos envíos de correos electrónicos desde correos de Promociones y Cobranzas Beta, dentro de los cuales parece que está el tuyo, me puedes por favor confirmar tu correo."

Víctima: "claro es jortiz@cobranzasbeta.com"

Atacante: "si efectivamente están saliendo correos desde tu cuenta, parece que está infectada con un virus tengo que revisar dentro de tu cuenta, me puedes por favor regalar tu contraseña para poder mirar."

Víctima: "si claro, mi contraseña es Mariana2005*"

Atacante: "me la puedes deletrear por favor"

Víctima: "sí, es m mayúscula, a, r, i, a, n, a, 2, 0, 1, 5, asterisco"

Atacante: "vale, voy a revisar y a quitar el virus, si no puedo me vuelvo a comunicar contigo para ver cómo podemos corregir el problema, muchas gracias por tu ayuda eres muy amable, que tengas un buen día"

Víctima: "gracias a ti, hasta luego"

Atacante: "gracias hasta luego"

7.5.2.3 Hallazgos encontrados y forma de mitigarlos en la prueba 1. Con este ataque se detectaron las siguientes falencias y la forma de mitigarlas; en el Cuadro 9. Pérdida del caller id original desde una línea externa, Cuadro 10. Divulgación de entrada y salida de personal a la empresa y Cuadro 11. Falta de capacitación del personal en ataques de ingeniería social se encuentran especificadas una a una las falencias de seguridad encontradas y la forma de mitigarlas.

Cuadro 9. Pérdida del caller id original desde una línea externa

Falencia de seguridad	Pérdida del caller id original desde una línea externa al momento de ser transferida a extensiones de regionales lo cual permite camuflar al atacante y presentarse como una llamada interna válida.
Forma de mitigar	Pasar el caller id de la llamada original de forma que la persona receptora de la misma pueda identificar si la llamada está siendo realizada de una extensión interna o un número telefónico externo.

Fuente: Diseñadores del proyecto.

Cuadro 10. Divulgación de entrada y salida de personal a la empresa

Falencia de seguridad	Ausencia de un proceso donde se informe de la entrada y salida de personas a la empresa; hace vulnerable a la compañía frente a suplantación de identidad; gracias a dicha carencia fue posible suplantar a una persona que no trabajaba en la empresa, de esta misma forma se puede suplantar personas recién ingresadas a la empresa o personas que recién salieron de la empresa.
Forma de mitigar	Una forma de mitigar este tipo de ataques es enviar masivamente un comunicado, cuando una persona ingresa o sale de la empresa por parte de recursos humanos, buscando avisar al personal dentro de la firma de dicha situación, este procedimiento tiene mayor valor cuando se retira personal administrativo, ya que son cargos con manejo de información más sensible.

Fuente: Diseñadores del proyecto.

Cuadro 11. Falta de capacitación del personal en ataques de ingeniería social

Falencia de seguridad	Necesidad de capacitación al personal en ataques de ingeniería social; las personas de la empresa no cuentan con el conocimiento necesario sobre dicha temática y posibles ataques de este tipo a los que pueden estar expuestas.
Forma de mitigar	El personal de Promociones & Cobranzas Beta debe recibir capacitación sobre cómo identificar ataques de ingeniería social, este tipo de capacitación debe ser impartida de forma continua y reforzando cada 6 meses con las últimas técnicas de esta temática; al final de las capacitaciones las personas deben ser capaces de detectar y reportar al departamento de sistemas, posibles incidentes de seguridad con respecto a ataques de ingeniería social.

Fuente: Diseñadores del proyecto.

7.5.2.4 Resultado de la prueba 2. Se logró solicitar el cambio de contraseñas de 10 usuarios en el área de sistemas, esto gracias a que los auxiliares de sistemas no siguieron el procedimiento establecido para desbloqueo de usuarios de dominio y correo. Las evidencias recolectadas son las grabaciones transcritas y las imágenes de los escritorios de los usuarios desbloqueados.

7.5.2.5 Transcripción llamada de ejemplo prueba 2. A continuación, un ejemplo mediante la transcripción de una llamada:

Víctima: "buenos días Promociones y Cobranzas Beta, le habla Natalia Tovar en que puedo colaborar."

Atacante: "hola Natalia, ¿cómo estás?, hablas con Enrique García, supervisor de Barranquilla, lo que sucede es que hoy llegué a trabajar y mi contraseña no funciona para entrar en el computador."

Víctima: "claro, Sr. García voy a resetear su contraseña; permítame un momento.... listo su nueva contraseña es Beta1234*, recuerde cambiarla cuando entre al computador"

Atacante: "gracias Natalia, que tenga buen día."

Víctima: "hasta luego buen día"

7.5.2.6 Hallazgos encontrados y formas de mitigarlos. En el Cuadro 12. Demora proceso aviso deshabilitación de usuarios y Cuadro 13. No cumplimiento de procedimientos de control de usuarios este ataque se detectaron las siguientes falencias y la forma de mitigarlas:

Cuadro 12. Demora proceso aviso deshabilitación de usuarios

Falencia de seguridad	Se evidencio una vulnerabilidad, al no estar en línea la comunicación de salida e ingreso de personal con el área de sistemas.
Forma de mitigar	Se debe buscar un mecanismo o diseñar el proceso para que el bloqueo de los usuarios que salen de las empresas se realice en el menor tiempo posible.

Fuente: Diseñadores del proyecto.

Cuadro 13. No cumplimiento de procedimientos de control de usuarios

Falencia de seguridad	El área de sistemas no cumple con los procedimientos para desbloqueo de usuarios y cambio de contraseñas, durante los ataques se desbloquearon y cambiaron contraseñas de usuarios sin tener un soporte; cualquier persona de sistemas puede generar un desbloqueo aumentando el riesgo ya que no existe un responsable directo identificado.
Forma de mitigar	Es necesario establecer un lineamiento en la política de seguridad de la información para que solo personal autorizado pueda realizar esta actividad, además de establecer dentro del proceso una forma de validación que permita corroborar que el solicitante del desbloqueo o cambio de contraseña es quien dice ser.

Fuente: Diseñadores del proyecto.

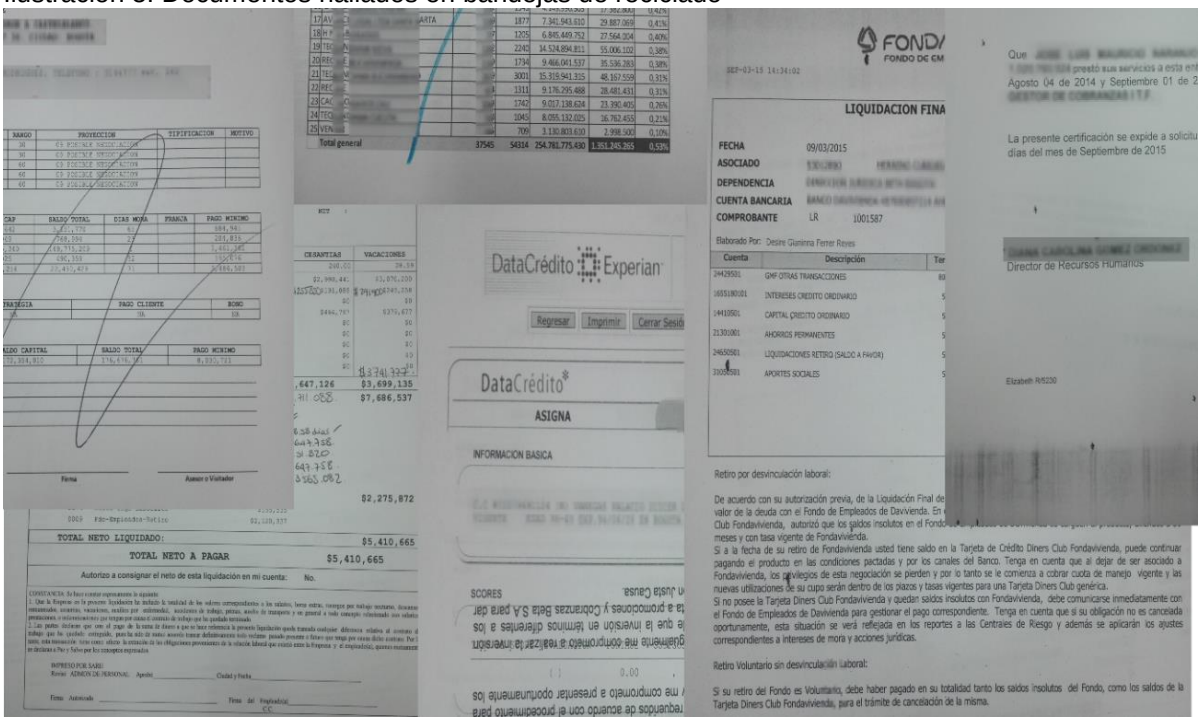
7.5.3 Dumpster diving o trashing (zambullida en la basura). Este ataque tiene como objetivo encontrar información en agendas telefónicas botadas, agendas de trabajo, papeles sueltos, extractos bancarios, cartas, unidades de almacenamiento como discos duros, usb's, dvd's entre muchas otras cosas arrojadas a la basura, gracias a esta técnica se encontró información de contraseñas de acceso a equipos de cómputo conectados a la red, contraseñas para acceder a aplicativos empresariales, información de despidos, extractos de ahorros, estados de cuenta de obligaciones, certificaciones de trabajo, liquidaciones por retiro a fondo de Davivienda, certificados de tradición, información de data crédito, liquidación de prestaciones, demandas realizadas, hipotecas, listas de clientes, actas cierre de mes regionales y actas de visitas; Esta información es información muy valiosa en las manos de un atacante, ya que tendría información confidencial de personas las cuales podrían ser un posible blanco para atacar con otras técnicas.

7.5.3.1 Resultado de la prueba. Se recolectaron documentos de las papeleras de reciclaje de las impresoras como lo son hojas abandonadas en la bandeja de salida de las mismas; también se encontraron documentos y papeles en las papeleras de reciclaje evidenciando mediante fotografías las diferentes hojas y post-it pegados en los puestos de trabajo los cuales contienen información de contraseñas y usuarios; a continuación, se relacionan los documentos encontrados con información relevante.

- Información de data crédito de personas con productos del banco.
- Liquidaciones del fondo de ahorro y vivienda.
- Estado de ganancias de casas de cobro externas.
- Cartas de renuncia de exempleados de la empresa.
- Contraseñas y usuarios de dominio.

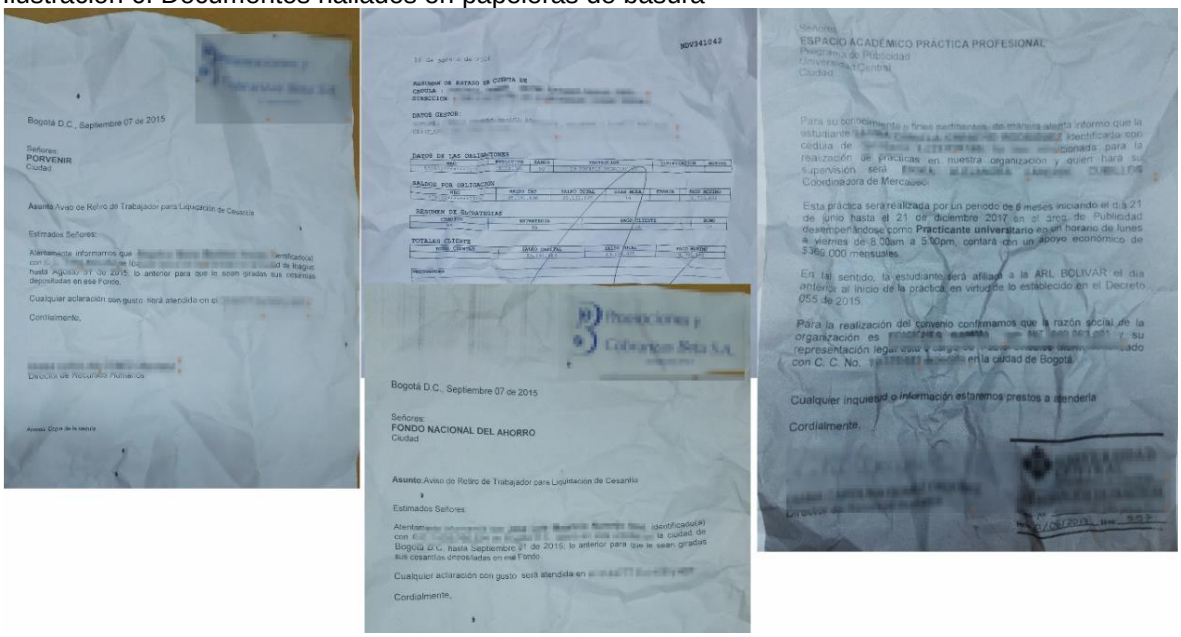
7.5.3.2 Imágenes de información recolectada, ejemplos. En la Ilustración 5. Documentos hallados en bandejas de reciclado, se puede visualizar un collage de papeles con información sensible encontradas en las bandejas de reciclaje; en la Ilustración 6. Documentos hallados en papeleras de basura, se evidencian documentos encontrados en las papeleras de basura.

Ilustración 5. Documentos hallados en bandejas de reciclado



Fuente: Diseñadores del proyecto.

Ilustración 6. Documentos hallados en papeleras de basura



Fuente: Diseñadores del proyecto.

7.5.3.3 Hallazgos encontrados y forma de mitigar. En este ataque se detectaron las siguientes falencias y la forma de mitigarlas:

Forma general de mitigar: identificar correctamente la información que es desechada o que sea usada como papel reciclado; la implementación de un DLP (Data Loss Prevention) ayuda a que la información confidencial no se fugue por medio de impresiones, usb, correos entre otros dispositivos; la implementación de políticas de manejo de documentos físicos y de seguridad informática ayudan a generar conciencia y prevenir que se tenga una mayor conciencia sobre la documentación que se desecha o descuida dentro de la empresa y en algunos casos fuera de ella.

En el Cuadro 14. Falta de control en el manejo de la información y el Cuadro 15. Inexistencia de una catalogación correcta de la información se describe en detalle las falencias encontradas en esta prueba y la forma de mitigarlas.

Cuadro 14. Falta de control en el manejo de la información

Falencia de seguridad	Ausencia de control en el manejo de la información, debido a que se permite dentro de la empresa imprimir cualquier tipo de información desde cualquier terminal, así mismo, es permitido enviar correos a cualquier destino sin filtrar el contenido adjunto.
Forma de mitigar	Crear una política empresarial para el manejo de la información, al igual que una política de seguridad a fin de ser estipulado y de conocimiento del personal, el manejo que deben de dar a recursos informáticos, documentos físicos, e información de la empresa tanto digital como física.

Fuente: Diseñadores del proyecto.

Cuadro 15. Inexistencia de una catalogación correcta de la información

Falencia de seguridad	No existe una catalogación correcta de la información que es crítica, publica, confidencial, externa, interna y personal; esto se evidencia al encontrar información de diferentes tipos entre ellos confidencial en hojas de papel reciclado.
Forma de mitigar	Crear un catálogo de información en donde se defina la importancia de los diferentes tipos de documentos e información que se manejan dentro de la empresa, de igual manera la implementación de picadoras de papel o cualquier otra forma de eliminación segura de documentos, esto es importante ya que no basta con rasgar el papel y arrojarlo a la basura, ya que sería fácilmente armado y leído, se debe picar el papel de forma que unirlo sea bastante complicado.

Fuente: Diseñadores del proyecto.

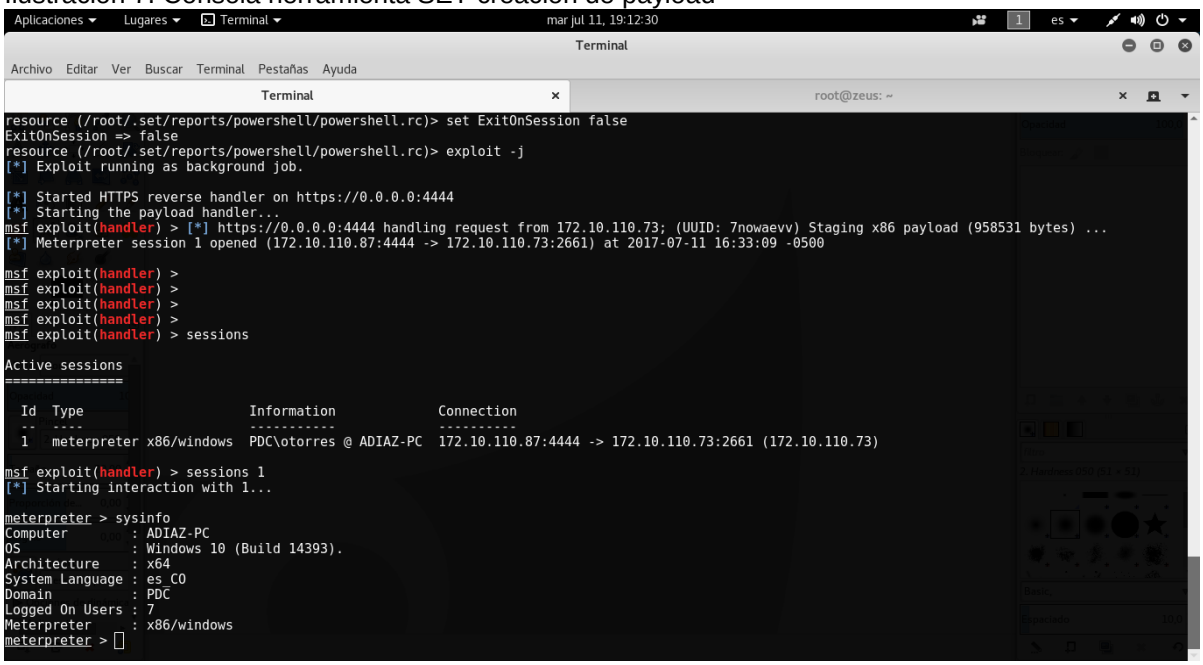
7.5.4 Ataques baiting (carnada). Regalos de medios extraíbles o encontrar estos casualmente. Este ataque aprovecha los perfiles de usuarios administradores, ya que busca activar un auto ejecutable y auto instalable con el fin de infectar equipos, abrir puertas traseras, instalar keylogger entre otras acciones maliciosas; se encontraron usuarios con permisos de administrador los cuales pueden permitir instalar software y modificar la configuración del sistema operativo; enviando un CD se entregó información sobre el sistema General de Riesgos Laborales lo cual es un tema en el cual se está capacitando al personal, junto con esta información se envió un archivo que al ser ejecutado permite tomar control del computador sin que el usuario se dé cuenta, en la Ilustración 7. Consola herramienta SET creación de payload, se puede apreciar la consola de SET la cual tiene una sesión activa de un equipo capturado con baiting.

7.5.4.1 Resultado de la prueba. Se enviaron 10 discos compactos con información del sistema general de riesgos laborales de la empresa, junto con el

autoejecutable (ejecutable.exe) el cual permite tomar control del computador en donde sea puesto el medio extraíble; se capturaron pantallazos de acceso a computadores tales como print screen de la pantalla y una foto desde la cámara web en los computadores que tenían webcam como se aprecia en la Ilustración 8. Captura camweb_snap.

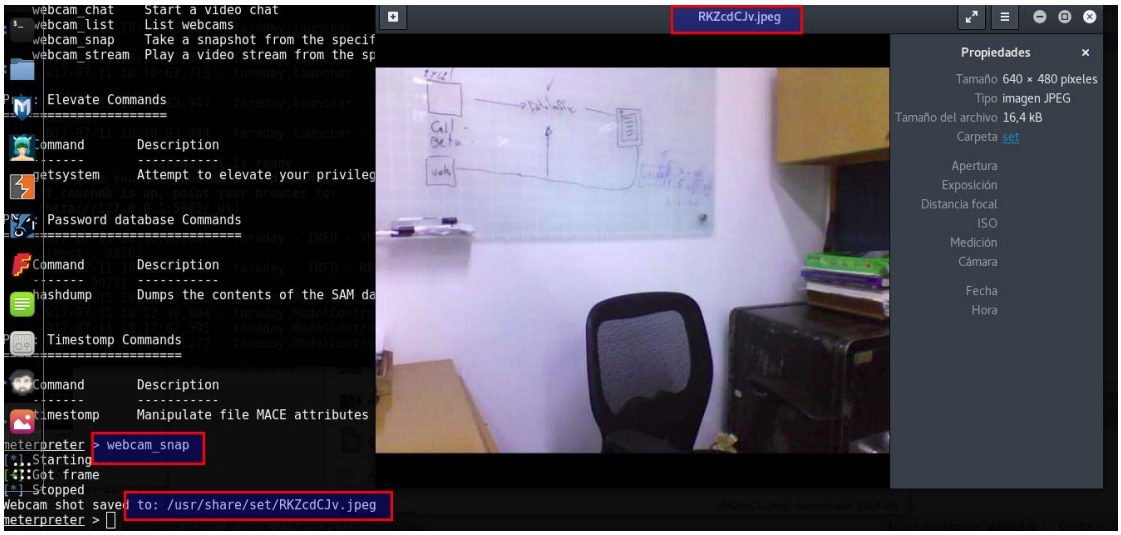
7.5.4.2 Imágenes ejemplo de la prueba. En la Ilustración 7. Consola herramienta SET creación de payload, se muestra una captura de pantalla de la consola de la herramienta SET funcionando para una de las pruebas que se realizaron con esta; en la Ilustración 8. Captura camweb_snap, se muestra un pantallazo de la captura de imágenes desde la cámara del equipo cliente accedido.

Ilustración 7. Consola herramienta SET creación de payload



Fuente: Diseñadores del proyecto.

Ilustración 8. Captura camweb_snap



Fuente: Diseñadores del proyecto.

7.5.4.3 Hallazgos encontrados y forma de mitigarlos. En el Cuadro 16. Usuarios con más permisos en red interna de los necesarios, Cuadro 17. Usuarios con permisos de acceso a internet sin ser necesarios, Cuadro 18. Demasiados administradores en el Controlador de Dominio (CD) y Cuadro 19. Administración de configuración de perfiles de usuarios del CD se especifica las falencias encontradas en la prueba y como mitigarlas.

Cuadro 16. Usuarios con más permisos en red interna de los necesarios

Falencia de seguridad	Se encuentran usuarios con permisos de administrador sin requerir del mismo.
Forma de mitigar	Es necesario validar los perfiles de los usuarios según su función en la empresa y las necesidades informáticas de dicho rol dentro de la misma, con la finalidad de comprobar quien cuenta con permisos de administrador y si realmente los necesita.

Fuente: Diseñadores del proyecto.

Cuadro 17. Usuarios con permisos de acceso a internet sin ser necesarios

Falencia de seguridad	Usuarios con permisos de internet extralimitados, es decir más permisos de los que requiere para desempeñar sus labores dentro de la empresa.
Forma de mitigar	Verificar los perfiles y dar los permisos necesarios para realizar su labor diaria, esto acorde a las funciones dentro de la compañía.

Fuente: Diseñadores del proyecto.

Cuadro 18. Demasiados administradores en el Controlador de Dominio

Falencia de seguridad	Falta de control en el dominio de Promociones y Cobranzas Beta, debido a que existen múltiples usuarios que disponen del perfil de administrador o en algunos casos de usuario de administrador del dominio.
Forma de mitigar	Se debe limitar el acceso a la administración del controlador de dominio (CD). Usuarios específicos que desempeñen roles de administración y tengan clara la importancia del mismo para con el CD, de igual forma el usuario administrador del CD debe ser custodiado y auditado por máximo dos personas dentro de la empresa las cuales no harán uso del mismo, exceptuando tareas exclusivamente administrativas en las que los usuarios creados con perfil de administrador no puedan realizar la actividad, (ejemplo: restauración de un controlador de dominio, acceso a las bases de datos de dominio para reparación de las mismas, entre otras), Adicionalmente debe existir dentro de la política de seguridad de la información un ítem que describa el uso del mismo y quienes y cuando deben cambiar contraseñas.

Fuente: Diseñadores del proyecto.

Cuadro 19. Administración de configuración de perfiles de usuarios del CD

Falencia de seguridad	Se realizan cambios no autorizados de configuraciones de perfiles de usuario sin validación, y sin contemplar seguimiento de una política de seguridad.
Forma de mitigar	Las configuraciones solo deben realizarlas los administradores del dominio y se debe implementar dentro de la política de seguridad de la información, que rol y bajo que parámetros se asignaran diferentes roles.

Fuente: Diseñadores del proyecto.

7.5.5 Phishing. Es una técnica muy utilizada en la ingeniería social la cual busca engañar a la víctima haciéndose pasar por una entidad o persona; este tipo de ataques se realiza por lo general con envíos masivos de correos los cuales contienen links o URL´s que llevan a páginas web fraudulentas; para esta prueba la metodología utilizada fue utilizar publicidad falsa de una empresa que presta servicios familiares y beneficios para los usuarios afiliados; la publicidad se envió por correo electrónico a la lista general que tiene la empresa y la cual se encuentra habilitada para enviar información masiva; la publicidad enviada tenía una imagen en la cual se adiciono una dirección de internet que al dar clic sobre la imagen se abría un formulario web que solicita datos básicos (nombre, apellido y correo), la web solicita diligenciar los datos a cambio de un beneficio y cuando la

persona da clic sobre la imagen se envía automáticamente la información básica del equipo como usuario red, nombre de dominio y la dirección IP.

7.5.5.1 Resultado de la prueba. De las 463 personas a las cuales se les está realizando la prueba de ingeniería social, Ingresaron a la página web falsa 76 personas de las cuales 23 llenaron los datos del formulario (nombre, apellido y correo); al ingresar al formulario automáticamente se capturo los datos de IP y nombre de pc, se relacionan las IP y los cargos de las personas que llenaron los datos del formulario y enviaron la información. Es posible evidenciar en el Cuadro 20. Listado víctimas Phishing el listado de los cargos y direcciones IP de quienes fueron víctimas del ataque en la prueba.

Cuadro 20. Listado víctimas Phishing

Ítem	**Dirección IP**	**Cargo**
1	172.10.4.23	Asesor de cobranzas
2	172.10.102.76	Analista visitas
3	172.10.107.45	Auxiliar de monitoreo
4	172.10.4.35	Asesor de cobranzas
5	172.10.6.24	Dependiente judicial
6	172.10.3.56	Visitador
7	172.10.3.121	Asesor de cobranzas
8	172.10.7.12	Abogado interno
9	172.10.101.73	Asesor de cobranzas
10	172.10.101.56	Asesor de cobranzas
11	172.10.107.23	Aprendiz Sena
12	172.10.104.90	Auxiliar administrativo
13	172.10.2.2	Auxiliar operativo
14	172.10.11.2	Auxiliar operativo
15	172.10.11.34	Asesor de cobranzas
16	172.10.21.45	Auxiliar jurídico
17	172.10.21.76	Abogado
18	172.10.25.9	Visitador
19	172.10.25.23	Asesor de cobranzas
20	172.10.9.2	Auxiliar de operativo
21	172.10.10.7	Asesor de cobranzas
22	172.10.17.2	Auxiliar operativo.
23	172.10.17.15	Asesor de cobranzas

Fuente: Diseñadores del proyecto.

7.5.5.2 Hallazgos encontrados y forma de mitigarlos. En el Cuadro 21. Desconocimiento del personal sobre este tipo de ataques, Cuadro 22. Desconocimiento del que hacer con emails que contienen phishing y Cuadro 23. Mal uso de la cuenta corporativa de correo electrónico se mencionan los hallazgos encontrados durante la prueba y la forma de mitigarlos.

Cuadro 21. Desconocimiento del personal sobre este tipo de ataques

Falencia de seguridad	Ausencia de capacitación a personal de la empresa en verificación de correos sospechosos.
Forma de mitigar	Capacitar a los empleados de la empresa en el reconocimiento de este tipo de correos maliciosos.

Fuente: Diseñadores del proyecto.

Cuadro 22. Desconocimiento del que hacer con emails que contienen phishing

Falencia de seguridad	Falta de conocimiento en cuanto a cómo se debe reportar un incidente de seguridad y a quien.
Forma de Mitigar	Capacitación en el reporte de incidencias.

Fuente: Diseñadores del proyecto.

Cuadro 23. Mal uso de la cuenta corporativa de correo electrónico

Falencia de seguridad	El mal uso de la cuenta de correo electrónico corporativa causa que el usuario interno y la empresa se enfrente contra correos basura y correos de phishing, es posible que en algún momento algún trabajador de la empresa se halla registrando en páginas de dudosa procedencia con el correo corporativo.
Forma de mitigar	Se debe capacitar al personal sobre las consecuencias de usar inadecuadamente las cuentas de correo; debe existir un lineamiento dentro de la política de seguridad de la información que haga referencia al uso inadecuado de la cuenta de correo electrónico corporativa.

Fuente: Diseñadores del proyecto.

7.5.6 Fuga de información por cuentas de correo (shoulder surfing). Durante las pruebas se usó la observación la cual hace parte de esta técnica; mediante la misma se evidencio que dentro de los correos de la empresa se guarda información importante sobre bases de datos, claves de usuarios, pantallazos de preguntas secretas, correos con información de clientes, entre otra información; se encontraron las siguientes vulnerabilidades, como se mostró anteriormente por medio de pretexting fue posible adquirir usuarios y contraseñas de personal, a

esto se suma que desde la red de internet es posible ingresar a la plataforma de correo ya que en esta no cuenta con restricción alguna para el ingreso, es decir, cualquier empleado de la compañía puede acceder desde internet y descargar la información que se encuentre almacenada; también se detectó que la página de correo no cuenta con un certificado de seguridad lo cual expone el canal de datos al no estar encriptada la comunicación.

Se evidencia que en el momento de una persona salir a vacaciones, de licencia o por cualquier otra circunstancia que amerite ausentarse de la empresa por un tiempo prolongado, los usuarios de autenticación de los diferentes aplicativos usados dentro de Promociones y Cobranzas Beta continúan activos; esta es una vulnerabilidad que permite hacer suplantación de usuarios.

También se detecta que algunos empleados de la empresa se ausentan de su lugar de trabajo dejando el equipo de cómputo sin bloqueo de escritorio dejando información y acceso a programas al alcance de posibles atacantes; a su vez se visualiza que en los escritorios de los computadores Windows se encuentran atestados de documentos y carpetas.

Es importante resaltar que esta técnica es solo mediante observación motivo por el cual solo fue posible ver por encima del hombro y hablando con personas sobre el contenido dentro de los correos. Buscando no pasar los límites de confidencialidad no se accedió a correos directamente para validar dicha información.

7.5.6.1 Hallazgos encontrados y formas de mitigarlos. En el Cuadro 24. Inexistencia de definición de uso de correo empresarial en Internet, Cuadro 25. Inexistencia de una herramienta que controles la fuga de información, Cuadro 26. Inexistencia de certificados de seguridad, Cuadro 27. Uso inadecuado de las herramientas informáticas, Cuadro 28. Inexistencia de configuración y política de intentos fallidos de contraseña, Cuadro 29. No cumplimiento en las políticas de seguridad informática, Cuadro 30. Definición de tiempo de bloqueo de pantalla por inactividad, Cuadro 31. Definición de des logueo o bloqueo de aplicativos por inactividad y Cuadro 32. Desconocimiento de la importancia de bloquear el equipo y des autenticarse de aplicaciones muestran las falencias detectadas mediante el ataque de shoulder surfing y la forma de mitigarlas:

Cuadro 24. Inexistencia de definición de uso de correo empresarial en Internet

Falencia de seguridad	La no existencia de una parametrización para los accesos al correo electrónico desde internet.
Forma de mitigar	Es necesario evaluar y permitir el acceso a las cuentas de correo desde internet solo al personal que necesita de dicha funcionalidad al igual que quien se encuentre autorizado por la gerencia para usar la misma, de igual manera es necesario que exista el lineamiento dentro de la política de seguridad de la empresa.

Fuente: Diseñadores del proyecto.

Cuadro 25. Inexistencia de una herramienta que controles la fuga de información

Falencia de seguridad	El no control y prevención de fuga de información por medios electrónicos o digitales.
Forma de mitigar	Implementar un DLP (Data Loss Prevention); dicha implantación mitiga considerablemente la fuga de información, además debe existir un direccionamiento sobre el uso de la información y las herramientas de trabajo en la política de seguridad de la información buscando el uso adecuado de los datos de la empresa.

Fuente: Diseñadores del proyecto.

Cuadro 26. Inexistencia de certificados de seguridad

Falencia de seguridad	La empresa no cuenta con un certificado de seguridad para la página web que provee el servicio de correo en internet.
Forma de mitigar	Es necesario habilitar un certificado de seguridad en el correo electrónico lo cual asegura el canal al encriptar la información previendo problemas de seguridad.

Fuente: Diseñadores del proyecto.

Cuadro 27. Uso inadecuado de las herramientas informáticas

Falencia de seguridad	El uso inadecuado de la herramienta de correo electrónico, archivos con bases de datos y aplicaciones se deben compartir por canales seguros.
Forma de mitigar	Implementar servidores de archivos o espacios en la nube en los cuales se pueda compartir información de forma segura, además de concientizar al personal sobre el uso de recursos informáticos.

Fuente: Diseñadores del proyecto.

Cuadro 28. Inexistencia de configuración y política de intentos fallidos de contraseña

Falencia de seguridad	Se detecta que no se encuentra configurada y parametrizada alguna estrategia para mitigar posibles ataques de diccionario o fuerza bruta, las cuentas de correo electrónico permiten múltiples intentos, sin bloquear al usuario o la dirección IP del atacante.
Forma de mitigar	Es necesario parametrizar las cuentas, con el fin de bloquear las mismas después de determinada cantidad de intentos, protegiendo de esta manera posibles ataques de fuerza bruta.

Fuente: Diseñadores del proyecto.

Cuadro 29. No cumplimiento en las políticas de seguridad informática

Falencia de seguridad	El compartir los usuarios de red afecta directamente la confidencialidad la cual hace referencia a la privacidad de la información almacenada y procesada en los diferentes equipos informáticos, es responsabilidad de cada usuario el manejo de sus credenciales de acceso, es decir, del usuario y contraseña necesarios para acceder a los diferentes sistemas informáticos de la compañía, las credenciales de acceso son personales e intransferibles.
Forma de mitigar	Capacitar al personal en la importancia de no prestar los usuarios bajo ninguna circunstancia, exceptuando que por escrito se deje constancia que se entrega para determinado uso; es de vital importancia desarrollar mecanismos que permitan detectar automáticamente cuando una persona se ausenta de la empresa por un tiempo prolongado, con esto se realizara el bloqueo de cuentas asignadas a el usuario así se mitigaran posibles accesos internos y externos en la ausencia del funcionario.

Fuente: Diseñadores del proyecto.

Cuadro 30. Definición de tiempo de bloqueo de pantalla por inactividad

Falencia de seguridad	Los bloqueos automáticos de los equipos por inactividad en las políticas del dominio tienen tiempos muy largos y en algunos casos no se aplican.
Forma de mitigar	Desde las políticas de dominio, es necesario parametrizar el bloqueo del equipo dentro del dominio, lo cual asegura que sea bloqueado el mismo automáticamente en un tiempo prudencial de inactividad, por si el usuario olvida bloquearlo.

Fuente: Diseñadores del proyecto.

Cuadro 31. Definición de desbloqueo o bloqueo de aplicativos por inactividad

Falencia de seguridad	Inexistencia de parametrización en bloqueo de aplicativos.
Forma de Mitigar	Se debe parametrizar los aplicativos para que estos se bloqueen automáticamente al dejar de usarlos por determinado tiempo, se recomienda que este tiempo no supere los 5 minutos de inactividad.

Fuente: Diseñadores del proyecto.

Cuadro 32**.** Desconocimiento de la importancia de bloquear el equipo y des autenticarse de aplicaciones

Falencia de seguridad	Desconocimiento de la importancia de bloquear el equipo o des autenticarse de las aplicaciones empresariales al momento en el que estos no van a ser usados.
Forma de mitigar	Capacitar a los empleados, es necesario concientizar e informar a los empleados en la importancia que tiene bloquear los equipos de cómputo al igual que des autenticarse de las aplicaciones empresariales al momento de dejar de usar estos, se recomienda hacer campañas lúdicas las cuales creen el hábito de bloquear los equipos de cómputo, al igual que utilizar métodos de recordación.

Fuente: Diseñadores del proyecto.

7.5.7 Tailgating. Se basa en solicitar ayuda de una persona autorizada para tener acceso a las áreas restringidas; en las pruebas realizadas a la empresa no fue posible explotar esta técnica de ingeniería social ya que desde la portería del edificio principal son muy estrictos con el ingreso de personal, sin embargo, se evidencio que las personas al ser autorizadas en portería para su ingreso deambulan libremente por el edificio, esto se presenta al ingresar a el edificio y dirigirse a la oficina con la cual se debe presentar, esto se repite cuando se finaliza la reunión y se dirige a la salida.

7.5.7.1 Hallazgos encontrados y formas de mitigarlos. En el Cuadro 33. Responsabilidad de invitados por parte del personal de la empresa se habla sobre el hallazgo encontrado y la forma de mitigarlo

Cuadro 33. Responsabilidad de invitados por parte del personal de la empresa

Falencia de seguridad	Al permitir ingresar personal ajeno a la empresa por autorización de un empleado, automáticamente queda bajo la responsabilidad del empleado el personal externo, lo que quiere decir que si se presenta cualquier anomalía en relación con la seguridad la persona que autorizo el ingreso responderá.
Forma de mitigar	Siempre que se autorice el ingreso de personal ajeno a la empresa se debe realizar el respectivo acompañamiento mientras este en las instalaciones de la empresa, si se llega a detectar personal sin identificación de la compañía (carne) que no esté acompañado de personal de la empresa se debe reportar a los guardas de seguridad o acompañarlo hasta la salida o a su destino siempre reportando el incidente en el área administrativa.

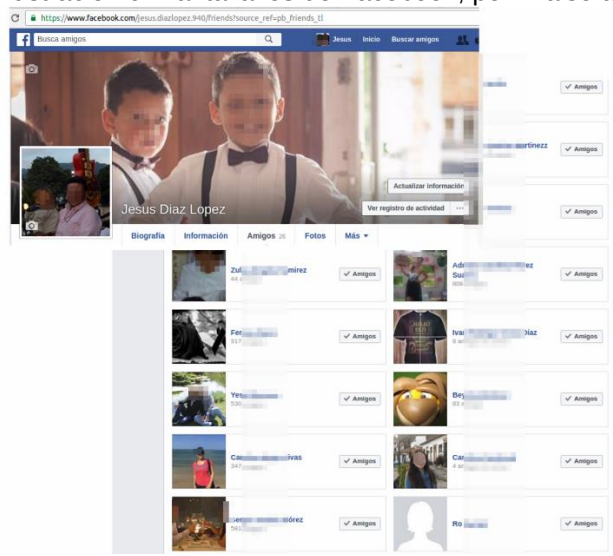
Fuente: Diseñadores del proyecto.

7.5.8 Ataque a redes sociales. Una de las fases de ataque de la ingeniería social es la recopilación de información con el fin de generar ataques organizados y muy entramados, donde tienen una gran cantidad de datos los cuales aumentan el éxito de un ataque dirigido; para esta prueba se creó una cuenta de Facebook falsa con un perfil de asesor de cobranzas donde se comenzó a agregar personas por medio del directorio telefónico de Beta, el cual se puede conseguir fácilmente en internet, a medida que las personas fueron aceptando las invitaciones de amistad se facilitó agregar a más personas ya que al ver que tenían amigos en común se genera mayor confianza y las personas terminan por no revisar los perfiles de Facebook y aceptar la invitación; después de tener varias personas es cuestión de tiempo recopilar información y diseñar el ataque a las personas seleccionadas.

7.5.8.1 Resultado Prueba Realizada. Para esta prueba se creó un perfil falso en Facebook el cual tenía perfil de asesor de cobranzas, se adjunta como evidencia pantallas capturadas en donde se evidencia que personal de Promociones y Cobranzas Beta aceptan la invitación del perfil falso.

7.5.8.2 Evidencia perfil Facebook. Captura de información personal de colaboradores de la compañía para plantear ataques más fuertes. A continuación, se muestra la Ilustración 9. Pantallazos de Facebook, perfil falso atacante y perfil víctima empleado de PYCB, la cual es un collage de captura de pantallas de ejemplo de información recolectada mediante investigación en Facebook.

Ilustración 9**.** Pantallazos de Facebook, perfil falso atacante y perfil víctima empleado de PYCB



Fuente: Diseñadores del proyecto.

7.5.8.3 Hallazgos encontrados y formas de mitigarlos. En el Cuadro 34. Falta de verificación de contactos se puede ver la falencia encontrada en esta prueba y la forma de mitigarla:

Cuadro 34**.** Falta de verificación de contactos

Falencia de seguridad	Los errores recurrentes en internet son los siguientes: no validar las páginas a las cuales ingresan, no validar las personas con las cuales interactúan en las redes sociales, no validar la información que se publica en internet y no validar quienes tienen acceso a dicha información, la falta de realizar este tipo de validaciones es la causa por la cual se puede estar expuesto a ataques informáticos, ya que al no revisar los certificados de seguridad de los sitios web se puede estar expuesto a técnicas como el phishing, al no revisar las solicitudes de amistad y no parametrizar correctamente las redes sociales es posible estar entregando acceso a información personal.
Forma de mitigar	La forma de mitigar este tipo de comportamientos es capacitar al personal en los diferentes riesgos que se tienen al navegar por internet, enseñar las diferentes técnicas con las cuales pueden ser atacados consiguiendo que se tome conciencia de los peligros que se corren al compartir información en la red.

Fuente: Diseñadores del proyecto.

7.6 ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 1

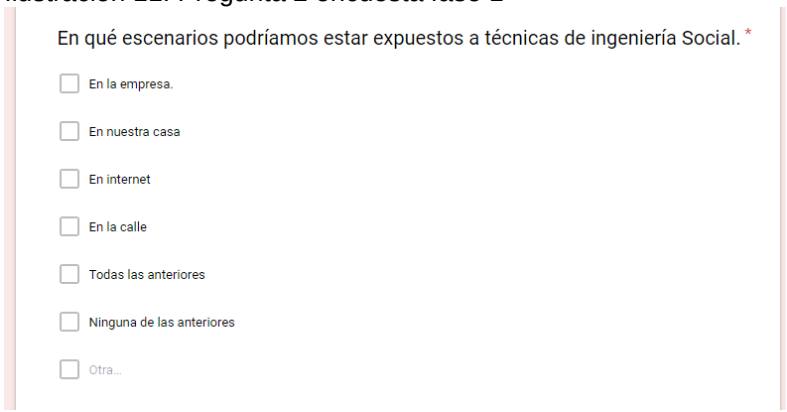
La primera fase del proyecto tiene como objetivo conocer el estado de consciencia y conocimiento de los empleados de Promociones y Cobranzas Beta acerca de la ingeniería social; para obtener esta información se decidió realizar una encuesta que toma un muestreo el cual permite comprender que tanto saben los trabajadores sobre el tema además de establecer un punto de partida sobre el nivel de percepción de seguridad frente a la temática que las personas tienen frente a este tipo de ataques.

Las Ilustración 10. Pregunta 1 Encuesta fase 1, Ilustración 11. Pregunta 2 Encuesta fase 1, Ilustración 12. Pregunta 3 Encuesta fase 1, Ilustración 13. Pregunta 4 Encuesta fase 1, Ilustración 14. Pregunta 5 Encuesta fase 1, Ilustración 15. Pregunta 6 Encuesta fase 1 e Ilustración 16. Pregunta 7 Encuesta fase 1, muestran el formato utilizado para el sondeo en la primera fase del proyecto; para realizar la encuesta se utilizó la herramienta Forms que ofrece Google gratuitamente y desde la cual se realizó el formulario; en esta primera serie de preguntas participaron 98 trabajadores lo cual representa el 21% de la población.

Ilustración 10. Pregunta 1 encuesta fase 1

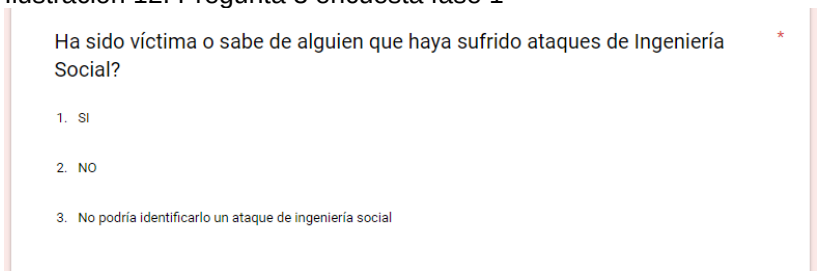
Fuente: Diseñadores del proyecto.

Ilustración 11. Pregunta 2 encuesta fase 1



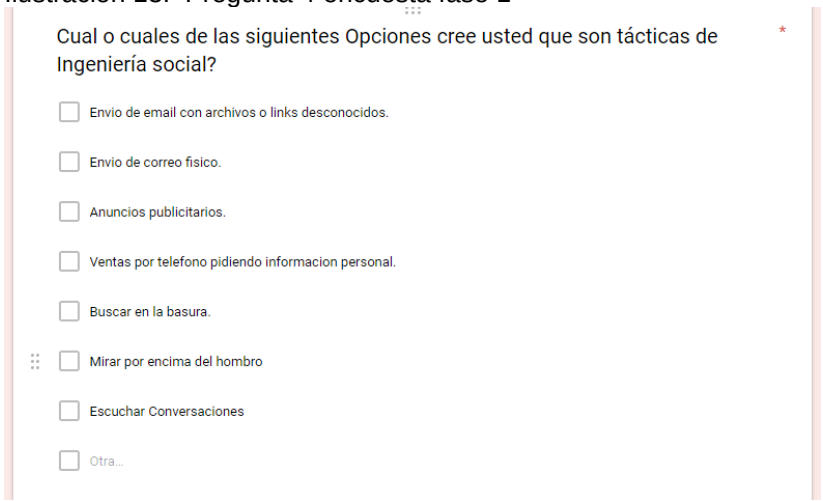
Fuente: Diseñadores del proyecto.

Ilustración 12. Pregunta 3 encuesta fase 1



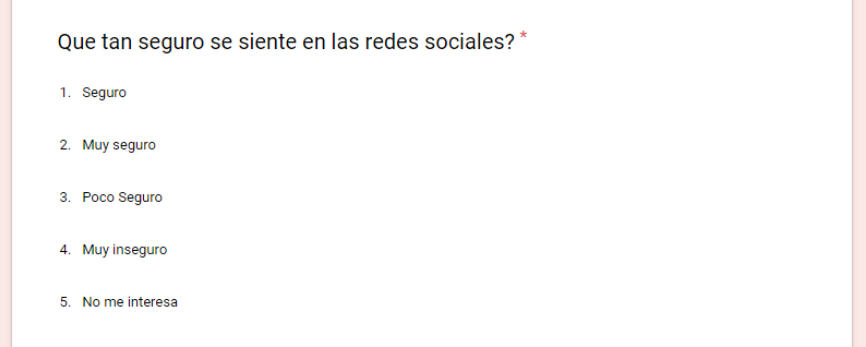
Fuente: Diseñadores del proyecto.

Ilustración 13. Pregunta 4 encuesta fase 1



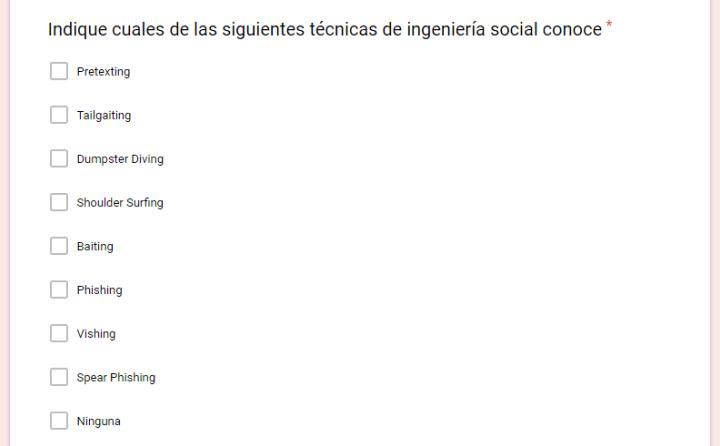
Fuente: Diseñadores del proyecto.

Ilustración 14. Pregunta 5 encuesta fase 1



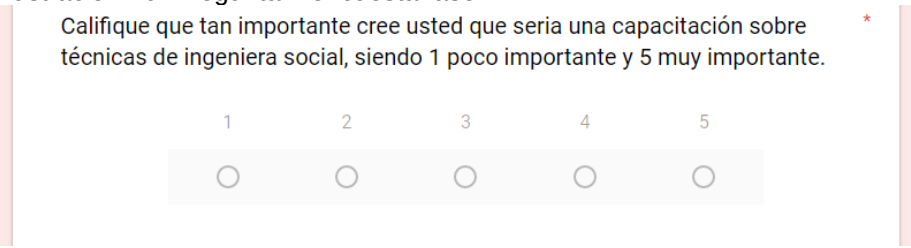
Fuente: Diseñadores del proyecto.

Ilustración 15. Pregunta 6 encuesta fase 1



Fuente: Diseñadores del proyecto.

Ilustración 16. Pregunta 7 encuesta fase 1

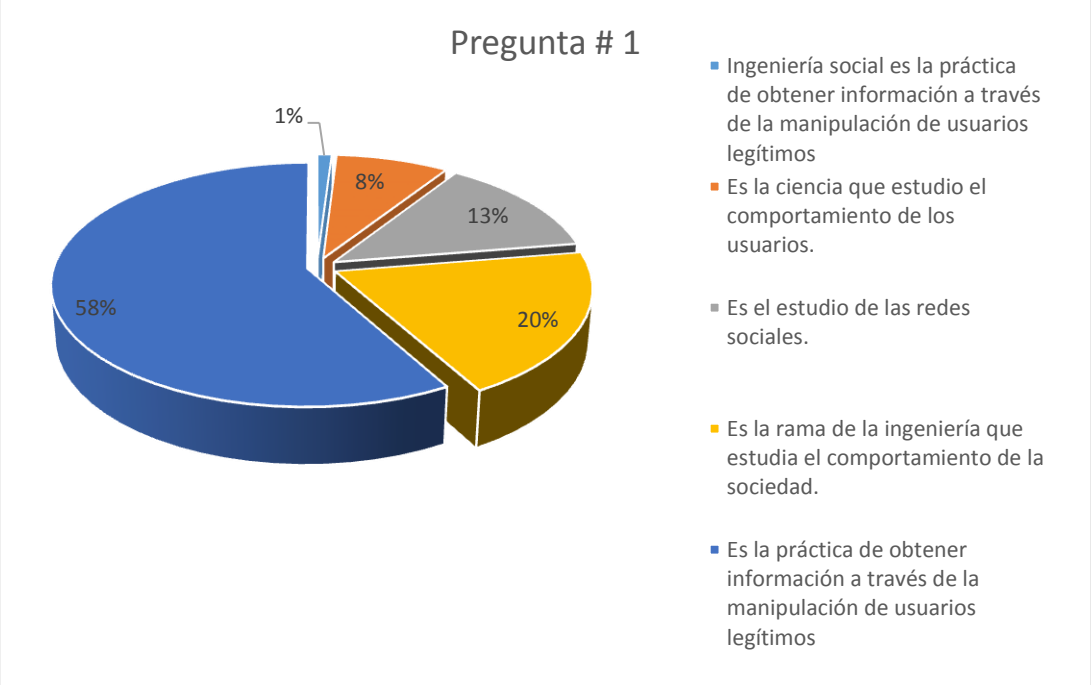


Fuente: Diseñadores del proyecto.

7.7 ANÁLISIS ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 1

7.7.1 Pregunta 1. ¿Qué es ingeniería social? con esta pregunta se busca determinar si los empleados tenían un concepto claro del significado ingeniería social; se observó que el 58% de las personas encuestadas entienden el significado del término; el 42% restante no tienen clara la definición o simplemente no saben que es; esto muestra la oportunidad de mejora en cuanto al aprendizaje del tema dentro de la compañía, capacitando al personal para generar mayor comprensión referente al asunto en cuestión y reforzar la temática, generando en ellos competencias que servirán para evidenciar posibles ataques de ingeniería social en su vida laboral y en su vida personal; en la Gráfica 1. Pregunta 1 fase, se puede ver en detalle estas cifras.

Gráfica 1. Pregunta 1 fase 1



Fuente: Diseñadores del proyecto.

7.7.1.2 Pregunta 2. ¿En qué escenarios podríamos estar expuestos a técnicas de ingeniería social? Esta pregunta busca determinar la consciencia de los colaboradores respecto al alcance que tiene la ingeniería social; en la Gráfica 2. Pregunta 2 Fase 1 de la Ilustración 18 podemos visualizar que el 76% de las personas son conscientes que pueden ser víctimas de técnicas de esta índole en

cualquier lugar, seguido de un 9% que piensa que solamente se puede estar expuesto al navegar en internet.

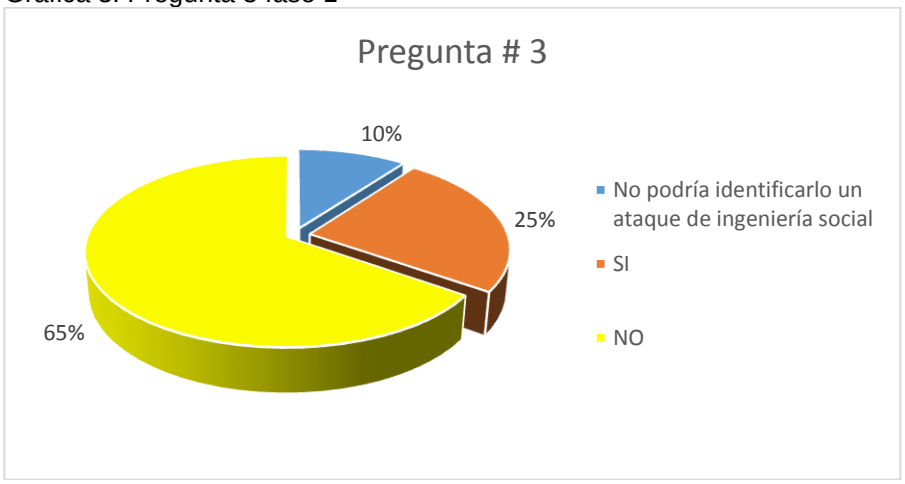
Gráfica 2.Pregunta 2 fase 1

Fuente: Diseñadores del proyecto.

7.7.1.3 Pregunta 3. ¿Ha sido víctima o sabe de alguien que haya sufrido ataques de ingeniería social? Por medio de esta pregunta se quiere saber si por experiencia propia o por historias de terceros los empleados han tenido algún tipo de aproximación con alguna de las técnicas que se utilizan en la ingeniería social; debido a que en este momento no se tienen claros los conceptos referentes al tema, ni sus técnicas de ataque se quiso indagar hasta qué punto las personas son capaces de identificar cuando son víctimas de estafas orquestadas a diferencia de otras como el mal llamado “raponazo” o robo a mano armada. La Gráfica 3. Pregunta 3 Fase 1, permite ver que el 65% de los encuestados afirma nunca haber pasado por este tipo de experiencia o haber escuchado de alguien que haya sido engañado mediante estos métodos; el 25% es consciente o sabe de

alguien que paso por un timo de esta índole; el 10% de los empleados no tiene claro cómo identificar un ataque de este tipo.

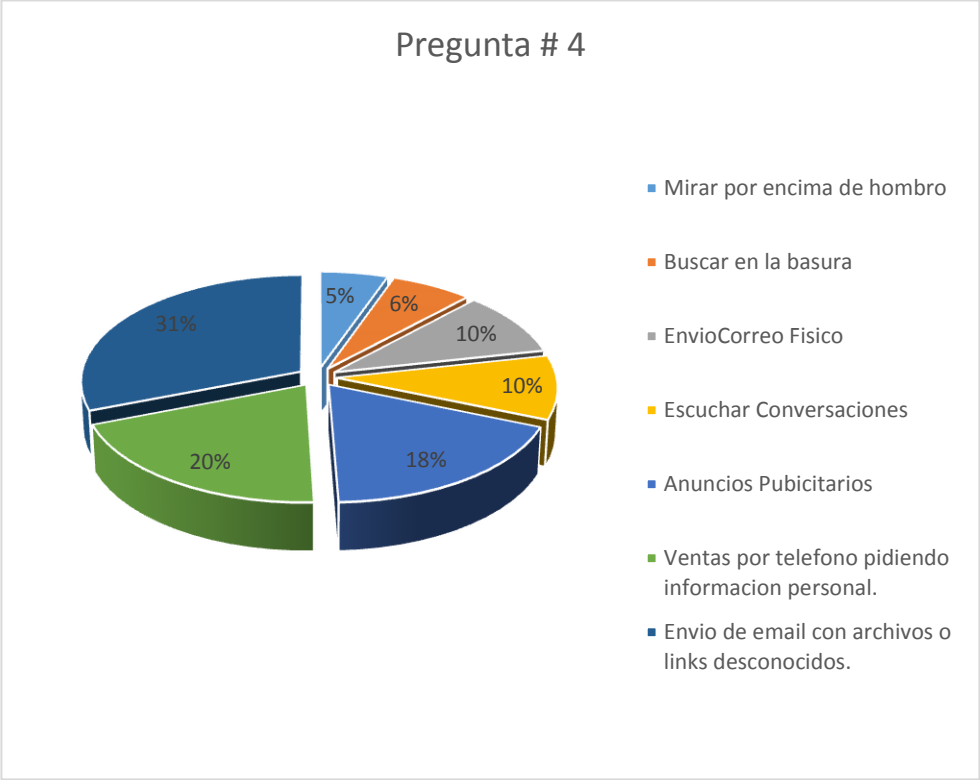
Gráfica 3. Pregunta 3 fase 1



Fuente: Diseñadores del proyecto.

7.7.1.4 Pregunta 4. ¿Cuál o cuáles de las siguientes opciones cree usted que son tácticas de ingeniería social? con esta pregunta se busca identificar la confianza existente en determinadas acciones cotidianas las cuales pueden ser un ataque de ingeniería social el cual se puede estar dejando pasar por alto y sin prestarle la debida atención; para este cuestionamiento en la Gráfica 4. Pregunta 4 Fase 1, se evidencia que el 31% de las personas indican ser conscientes de correos electrónicos con vínculos a otras páginas o con descarga de archivos que pueden ser potencialmente peligrosos; seguido por el 20% quienes piensan que las llamadas telefónicas en las que solicitan información personal pueden ser estafas; y el 18% desconfía de anuncios publicitarios. Adicionalmente se observa que las técnicas más identificadas son las que a menudo se anuncian por medios de comunicación como la televisión o la radio

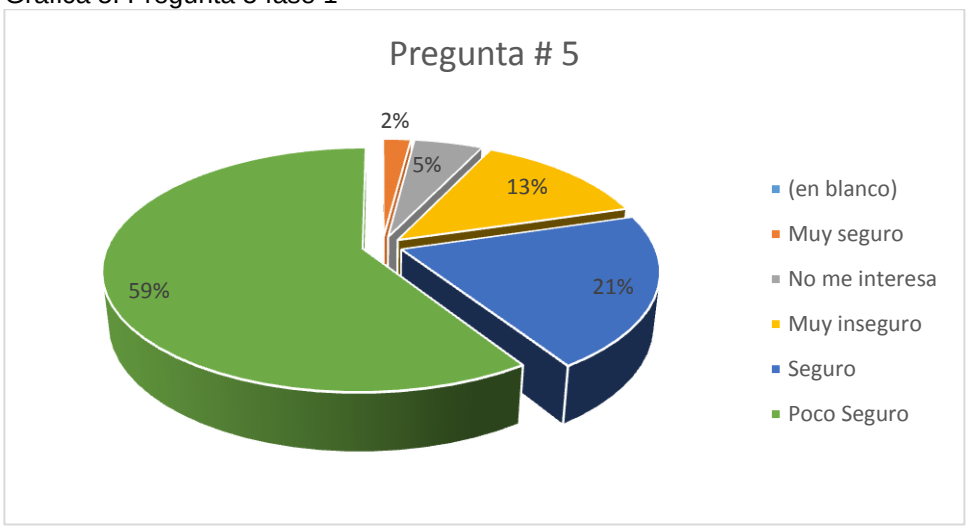
Gráfica 4. Pregunta 4 fase 1



Fuente: Diseñadores del proyecto.

7.7.1.5 Pregunta 5. ¿Qué tan seguro se siente en las redes sociales? Con este incognito se busca identificar que tan cuidadosos son los trabajadores con los peligros a los cuales están expuestos al navegar por las diferentes redes sociales; esta información es importante ya que muchas personas en general pasan una gran parte del tiempo en las redes sociales con lo cual existe una exposición a ataques de esta índole; por otra parte, se busca indagar acerca de la percepción de seguridad que se tiene sobre este medio de comunicación; la Gráfica 5. Pregunta 5 Fase 1, indica que el 59% de quienes respondieron la pregunta se sienten poco seguras en estos medios; el 13% se encuentran muy inseguros; el 5% no les interesa el tema de la seguridad; el 2% piensa que está muy seguro; y un 21% se consideran seguros en estas redes; lo que deduce que la percepción de inseguridad es mayor que la percepción de seguridad y algunas de las personas que se sienten seguras en las redes sociales realmente desconocen de las amenazas a las cuales pueden estar expuestos en ellas.

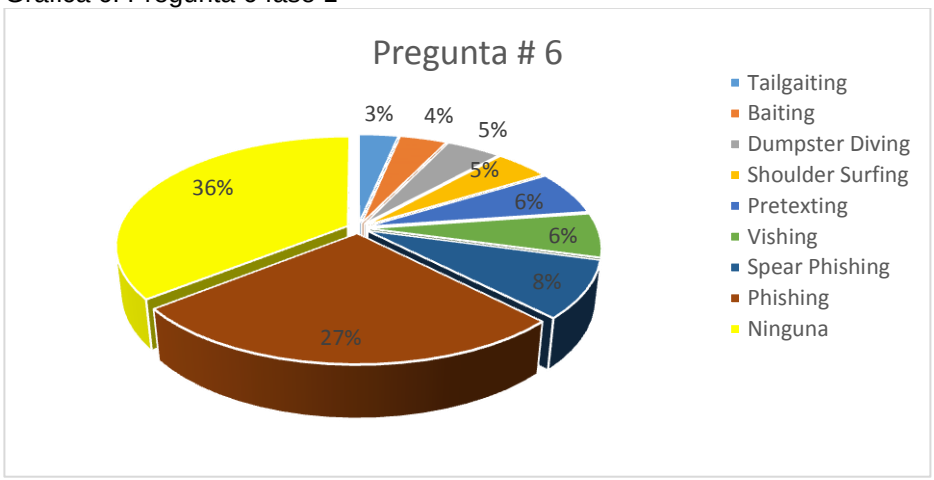
Gráfica 5. Pregunta 5 fase 1



Fuente: Diseñadores del proyecto.

7.7.1.6 Pregunta 6. Indique cuales de las siguientes técnicas de ingeniería social conoce. Mediante esta pregunta se quiere identificar que técnica de esta temática es la más reconocida y que tanto se desconoce acerca de estas permitiendo focalizar el plan de concientización; en la Gráfica 6. Pregunta 6 Fase 1, se puede apreciar que el 36% de las personas encuestadas desconoce por completo de estas; y la técnica más conocida es el Phishing ya que el 27% afirmo conocerla.

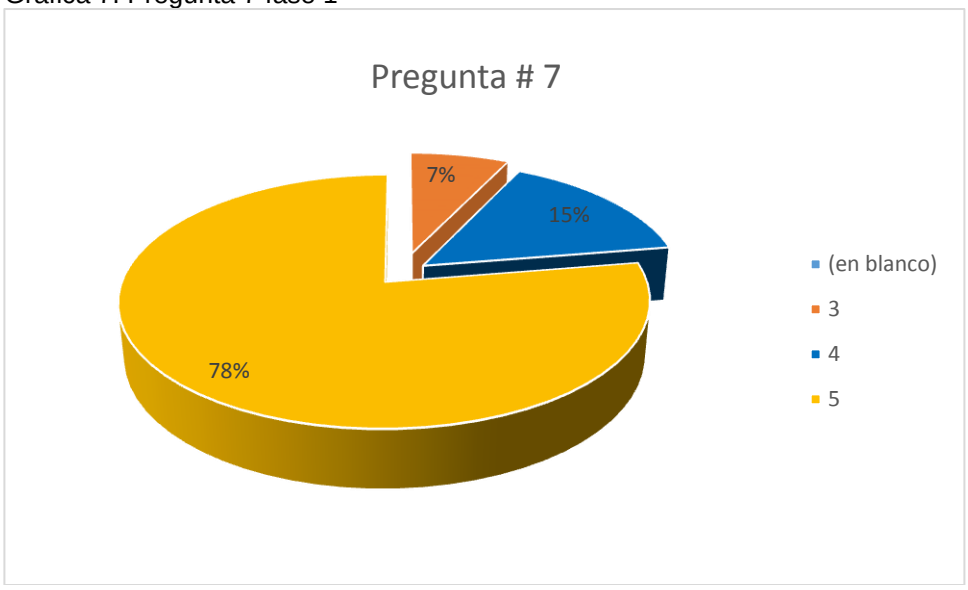
Gráfica 6. Pregunta 6 fase 1



Fuente: Diseñadores del proyecto.

7.7.1.7 Pregunta 7. Califique que tan importante cree usted que sería una capacitación sobre técnicas de ingeniera social, siendo 1 poco importante y 5 muy importante. Con esta pregunta se busca evaluar el grado de aceptación que las personas tienen para capacitarse en temas nuevos; en la Gráfica 7. Pregunta 7 fase 1, se puede ver que los empleados son conscientes de la importancia que tiene capacitarse en temas de seguridad, el 78% de los encuestados determino que es muy importante; el 15% indica que es bueno capacitarse en temas nuevos; el 7% tiene un punto de vista neutro con referente al tema y ninguna persona estuvo apática al tema de las capacitaciones; lo cual muestra aceptación para este tipo de capacitaciones.

Gráfica 7. Pregunta 7 fase 1



Fuente: Diseñadores del proyecto.

8. FASE 2 – EJECUCIÓN PLAN DE CONCIENTIZACIÓN

Para el diseño del plan de capacitación se tuvo en cuenta los análisis de la recolección de la información en las encuestas y pruebas de ingeniería social realizadas en la fase 1; basándose en esta premisa se describe en los sub niveles de ítem 8 las actividades a realizar y con las cuales se informa a los colaboradores de la compañía sobre la temática.

8.1 ¿QUÉ SE BUSCA CON ESTE PLAN CONCIENTIZACIÓN?

Acorde a las necesidades específicas definidas con el director del área de sistemas de Promociones y Cobranzas Beta S.A., visibles en el Anexo B. Acta de reunión 2, se llevarán a cabo los siguientes objetivos con el fin de cumplir con las mismas. A continuación, se definen las metas propuestas a cumplir.

- Generar recordación del tema ingeniería social que permita a los empleados de Promociones y Cobranzas Beta S.A., proteger la integridad de las personas e información de la entidad en forma adecuada.
- Capacitación didáctica y práctica, sobre ingeniería social para la mayor cantidad posible de personal en Promociones y Cobranzas Beta S.A., donde se explica y ayuda a responder a los asistentes las siguientes preguntas: ¿qué es la ingeniería social?, ¿cuáles son los ataques comunes de ingeniería social a los que se pueden encontrar expuestos?, y se entregan buenas prácticas que permiten identificar cuando pueden ser posibles víctimas de un ataque de ingeniería social.
- Diseñar 5 correos electrónicos de muestra, relacionados con reflexión de ingeniería social y enviar por lo menos dos durante la ejecución del plan.
- Entregar 2 afiches publicitarios que recuerden que se puede estar expuesto en diversas circunstancias y ser posible víctima de un ataque de ingeniería social, publicar uno para cada una de las sedes de la compañía, el cual será puesto en las carteleras informativas.
- Entregar instructivo en forma de presentación que permita a empleados que no tomen la capacitación presencial ver dicho documento y comprender el tema, además de contar con recomendaciones las cuales brindan recordación sobre la ingeniería social al personal de Promociones y Cobranzas Beta S.A., tanto nuevo como antiguo.

8.2 ALCANCE

El plan de concientización frente a la ingeniería social diseñado para Promociones y Cobranzas Beta S.A. busca preparar al personal de la organización frente a posibles ataques en esta rama de la seguridad generando conocimiento y recordación en el personal de la empresa; este contempla lineamientos base de la

temática y su desarrollo permite a los empleados disponer de conocimiento necesario para incrementar la habilidad de percepción frente a este tipo de ataques.

La metodología definida para la ejecución de este proyecto se encuentra establecido acorde a las prioridades de Promociones y Cobranzas Beta S.A. al igual que el desarrollo del plan de concientización se apoya en las capacidades con las que cuenta la compañía para enfrentar este tipo de situaciones que amenazan o afectan la integridad de sus empleados y la información de la empresa.

Se ha establecido con el área de Sistemas entregar una capacitación inicial sobre la temática para al menos el 80% de los colaboradores es decir 370 personas; la capacitación será de carácter obligatorio y el personal de la firma podrá asistir presencialmente o también recibirla mediante la herramienta Moodle reproduciendo un video; el video de capacitación a su vez será aprovechado para futuras oportunidades con personal nuevo, además se usaran mecanismos de recordación sobre la temática como apoyo del área de sistemas en temas de seguridad informática en este aspecto; afiches de concientización y correos electrónicos delimitados en los objetivos específicos de este documento, instructivo de recomendaciones para prevenir e identificar posibles ataques y cómo actuar frente a los mismos.

8.3 CAPACITACIÓN

Acorde a las necesidades detectadas se establecieron los siguientes métodos de capacitación:

8.3.1 Capacitación presencial.

Se definió para la sede Bogotá buscando una gran asistencia parte de los empleados de Promociones y Cobranzas Beta que se encuentra en esta sede ya que aloja a 213 empleados; esta capacitación busca informar a los colaboradores de la firma frente a los diversos métodos utilizados por atacantes informáticos para obtener datos sensibles, durante la cual se expondrán ejemplos de reflexión y entendimiento de la ingeniería social y como puede ser usada por ciberdelincuentes.

Dicha capacitación fue realizada con una duración de 1 hora, y se manejó la siguiente temática o contenido en la misma

- ¿Qué es ingeniería social?
- Definiciones.
- Objetivos.
- ¿Cuáles son las técnicas de ingeniería social?

- Baiting.
- Pretexting.
- Dumpster diving.
- Shoulder surfing.
- Tailgating.
- Phishing.
- Ciber bullying
- Happy slapping.
- Sexting.
- Sextorsion.
- Grooming.
- Ejemplos.
- Recomendaciones para hacer frente a la ingeniería social.

A esta capacitación presencial asistieron 123 personas, lo cual comprende el 57% de la población esperada para esta capacitación.

Luego de entregada la capacitación, en la Fase 3 se medirá el impacto generado en los trabajadores mediante otra encuesta y pruebas de ingeniería social.

La capacitación presencial lleva de la mano las firmas de asistencia que se encuentran en el Anexo G. Listas de asistencia.

8.3.2 Video de capacitación. Con la ayuda del área de comunicaciones y staff de Promociones y Cobranzas Beta se produce un video el cual abarca los temas de la capacitación presencial en un lapso de 20 minutos y tiene como objetivo llegar a los funcionarios de las sedes de: regional Armenia, regional Barranquilla, regional Bucaramanga, regional Cali, regional Cartagena, regional Cúcuta, regional Ibagué, regional Manizales, regional Medellín, regional Montería, regional Neiva, regional Pasto, regional Pereira, regional Santa Marta, regional Tunja, regional Valledupar y regional Villavicencio, los cuales abarcarían 250 personas; de esta manera los colaboradores en las sedes mencionadas reciben la información y se enteran de la problemática además de aprovechar el medio de comunicación para que nuevos empleados conozcan del tema o quienes quieran repasar puedan realizarlo de una forma sencilla.

Este video se presenta a modo de capacitación presencial, los asistentes deben diligenciar una lista de asistencia, a este modelo de capacitación asistieron 193 trabajadores, lo cual representa el 77,2 % de la población esperada.

En la Ilustración 17. Video ingeniería social Promociones y Cobranzas Beta, es posible visualizar un collage de varios pantallazos del video de capacitación realizado para este plan de concientización.

Ilustración 17. Video ingeniería social Promociones y Cobranzas Beta

Fuente: Diseñadores del proyecto.

Luego de confirmar que en las sedes mencionadas se visualizó el video de capacitación; en la Fase 3 se medirá el impacto generado por esta capacitación mediante otra encuesta y pruebas de ingeniería social.

8.3.3 Manual. El manual de concientización se encuentra en forma de presentación teniendo como fin facilitar futuras capacitaciones presenciales además de posibilitar el uso y lectura de cada uno de los empleados sirviendo de esta manera como un material de apoyo y recordación para el 100% de los empleados de la compañía, el cual no busca en futuro realizar una medición, pero si ayudar a reforzar conocimientos en la temática.

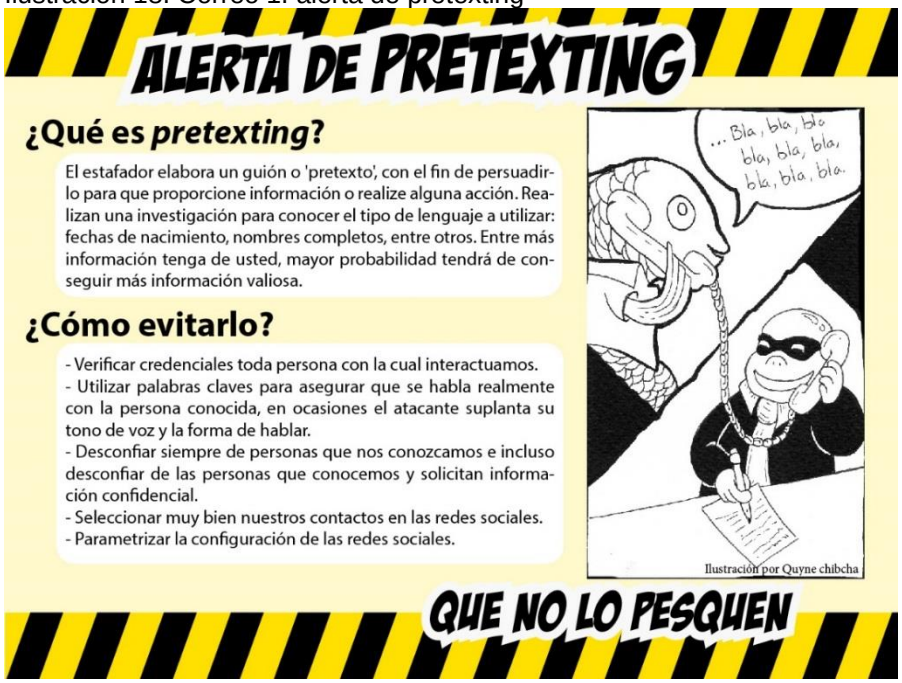
El manual se encuentra en el Anexo H. Manual presentación concientización ingeniería social Beta. Por solicitud de Promociones y Cobranzas Beta, se realizó en forma de presentación buscando dar utilidad para capacitaciones a la vez que auto estudio.

8.4 CONTINUIDAD Y RECORDACIÓN

Para generar recordación y dar una continuidad dentro de la empresa para que los colaboradores estén enterados de la problemática a la que se enfrentan se propone el siguiente material para que sea tenido en cuenta y de esta manera la firma pueda recordar a sus empleados la importancia de hacer frente a estos posibles ataques; Este material está disponible para el 100% de los empleados de promociones y Cobranzas Beta, y no busca realizar una medición de conocimiento e impacto, si no actuar como un material de apoyo en la recordación del tema; para ello se destinaron los siguientes recursos.

8.4.1 Correos electrónicos. Según el acta 3, la cual se encuentra disponible en el Anexo C. Acta de reunión 3, se aprobó 5 ejemplos de correos electrónicos, que enfocan recordación sobre el tema de ingeniería social y los ataques frecuentes, los cuales usara el área de sistemas como material de apoyo para enviarlos masivamente a los trabajadores de Promociones y Cobranzas Beta; a continuación, en la ilustración 18. Correo 1. alerta de pretexting, ilustración 19. Correo 2. alerta de dumpster diving, Ilustración 20. Correo 3. alerta de phising, ilustración 21. Correo 4. alerta de shoulder surfing e ilustración 22. Correo 5. alerta de tailgating se muestran imágenes de los correos aprobados.

Ilustración 18. Correo 1. alerta de pretexting

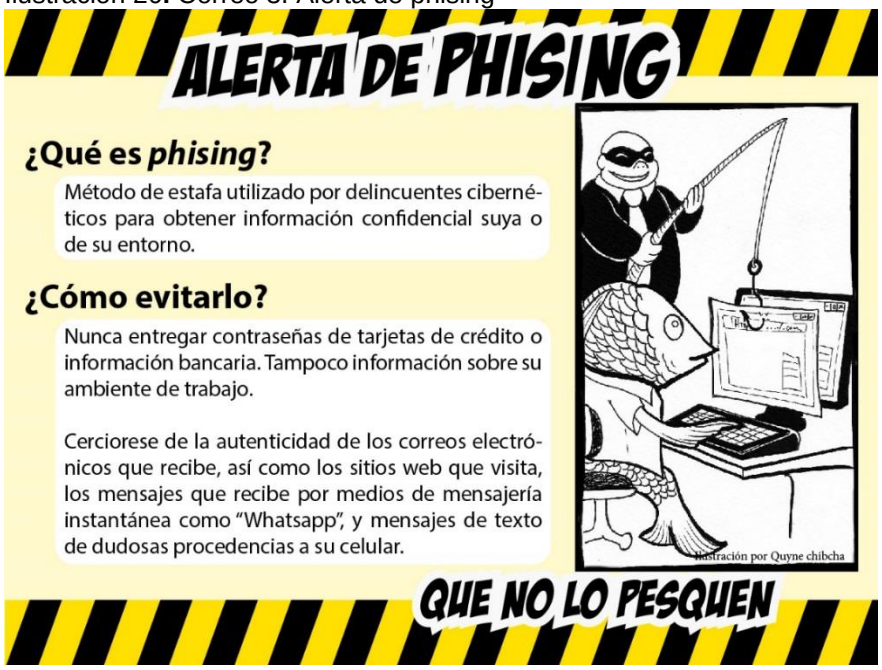


Fuente: Diseñadores del proyecto.

Ilustración 19. Correo 2. Alerta de dumpster diving

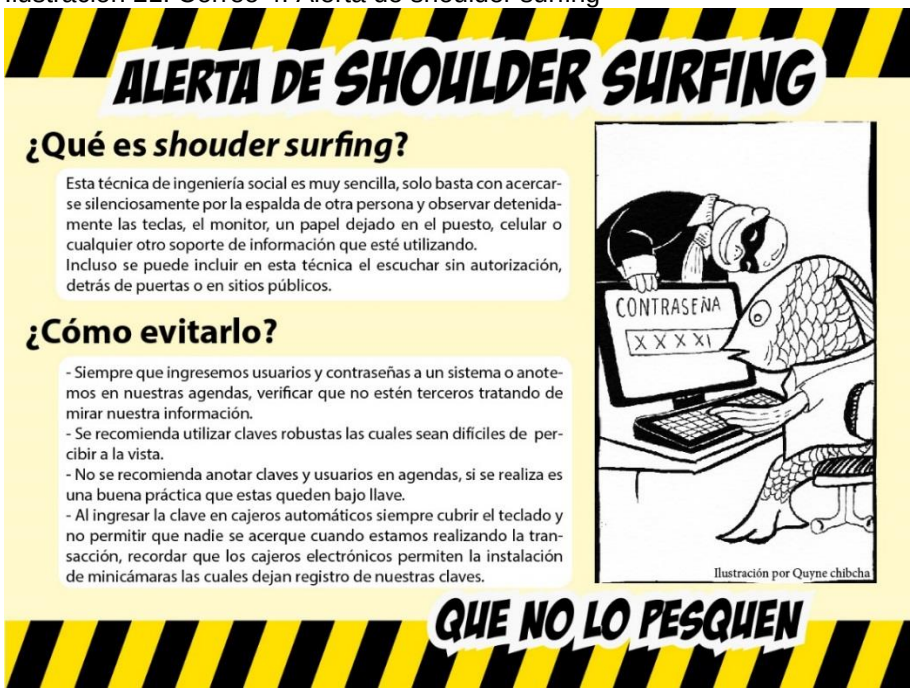
Fuente: Diseñadores del proyecto.

Ilustración 20**.** Correo 3. Alerta de phising



Fuente: Diseñadores del proyecto.

Ilustración 21. Correo 4. Alerta de shoulder surfing



Fuente: Diseñadores del proyecto.

Ilustración 22. Correo 5. Alerta de tailgating

Fuente: Diseñadores del proyecto.

8.4.2 Afiches publicitarios. 2 afiches publicitarios que serán usados en las carteleras de cada sede como apoyo de recordación del tema los cuales están disponibles para todos los empleados de la compañía como apoyo visual y de recordación; la Ilustración 23. Afiche 1 e Ilustración 24. Afiche 2 son imágenes de los afiches entregados.

Ilustración 23. Afiche 1

Fuente: Diseñadores del proyecto.

Ilustración 24. Afiche 2

Fuente: Diseñadores del proyecto.

8.5 RECOMENDACIONES DE GOBIERNO Y CONTINUIDAD

El objetivo de la administración de continuidad del plan de concientización es crear conciencia en los empleados de Promociones y Cobranzas Beta S.A buscando que conozcan de una manera general que es la ingeniería social, como es usada por los atacantes, que tipos de ataques son más frecuentes, además de buenas

prácticas, en donde se puedan identificar posibles ataques de ingeniería social buscando planificar las acciones necesarias para responder de forma adecuada ante un posible ataque de esta índole desde el momento en el que se detecte el mismo hasta la vuelta a la normalidad buscando repeler este de forma que posibles riesgos de seguridad sean reducidos al mínimo en el personal y sobre el negocio. Dichos lineamientos se sustentan en un conjunto de principios según las necesidades del negocio y en el entendimiento de riesgos asociados, y estos son:

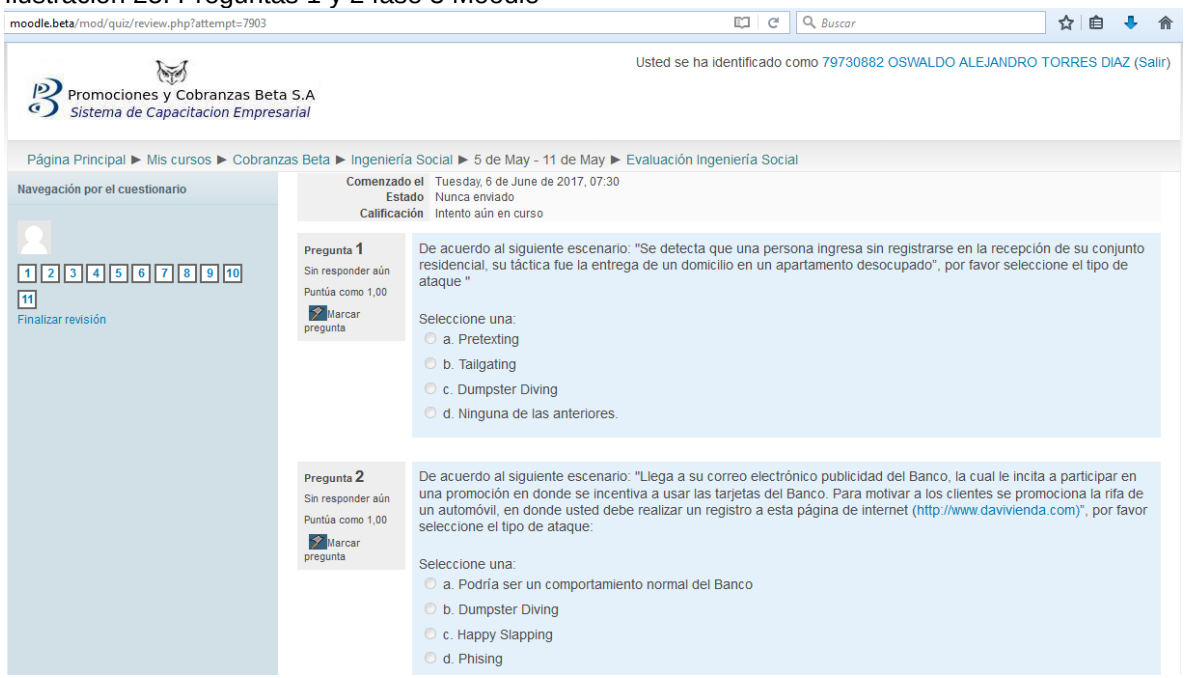
- El plan de concientización frente a la ingeniería social está orientado a proteger a los empleados de la empresa, así como preservar la información de la compañía.
- Todo el personal de Promociones y Cobranzas Beta S.A. debe ser capacitado y entrenado en los conocimientos base de ingeniería social y acciones a seguir en caso de un ataque.
- Conocer claramente los roles y responsabilidades que le competen en el marco de seguridad informática dentro de la empresa, mediante labores periódicas de formación y divulgación.
- En caso de presentarse un incidente de seguridad informática significativo en el que se detecte un ataque de ingeniería social se deben aplicar los mecanismos de comunicación apropiados con el área de sistemas, quien debe encargarse de la situación.
- El plan de concientización debe mantenerse actualizado, motivo por el cual se debe desarrollar, probar y de ser necesario mejorar de forma periódica ante cambios significativos y actualizaciones en temas de ingeniería social frente a nuevos métodos o estrategias que se detecten o evidencien en la sociedad, siendo necesario que en dicha revisión participe necesariamente el responsable de seguridad informática y directivos de la empresa.

9. FASE 3 - ANÁLISIS ESTADO LUEGO DE EJECUTAR EL PLAN DE CONCIENTIZACIÓN

9.1 ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 3

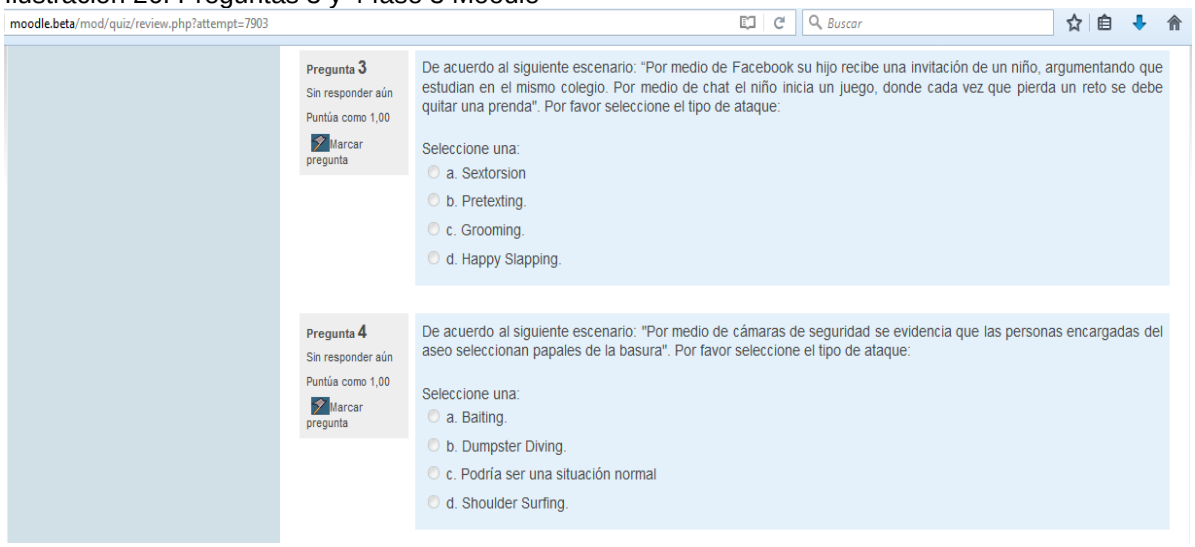
Las Ilustración 25. Preguntas 1 y 2 fase 3 Moodle, Ilustración 26. Preguntas 3 y 4 Fase 3 Moodle, Ilustración 27. Preguntas 5 y 6 fase 3 Moodle, Ilustración 28. Preguntas 7 y 8 fase 3 Moodle e Ilustración 29. Preguntas 9 y 10 fase 3 Moodle muestran el formato utilizado para realizar la encuesta sobre ingeniería social para la fase 2; se utilizó la herramienta Moodle la cual permite verificar que usuarios presentaron la encuesta y cuál fue su calificación.

Ilustración 25. Preguntas 1 y 2 fase 3 Moodle



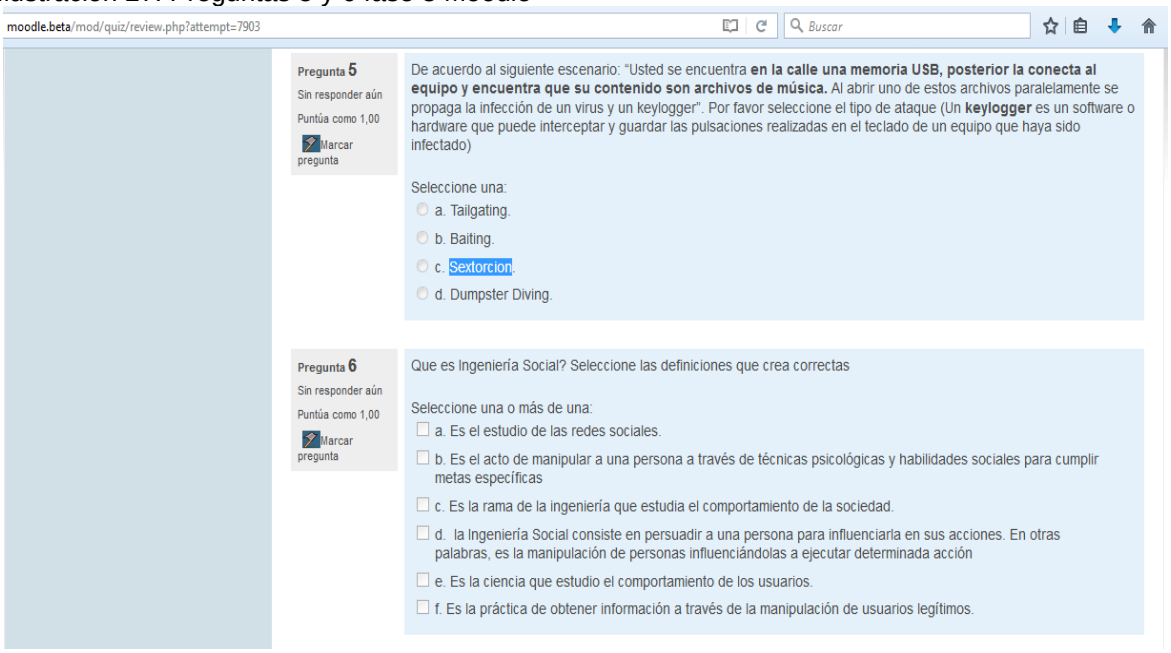
Fuente: Diseñadores del proyecto.

Ilustración 26. Preguntas 3 y 4 fase 3 Moodle



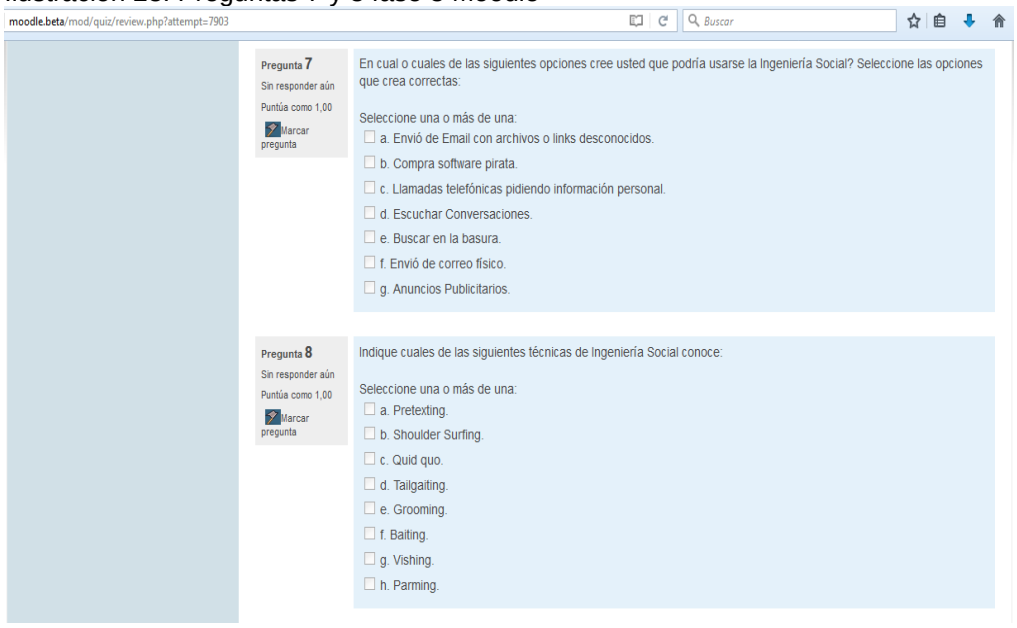
Fuente: Diseñadores del proyecto.

Ilustración 27. Preguntas 5 y 6 fase 3 Moodle



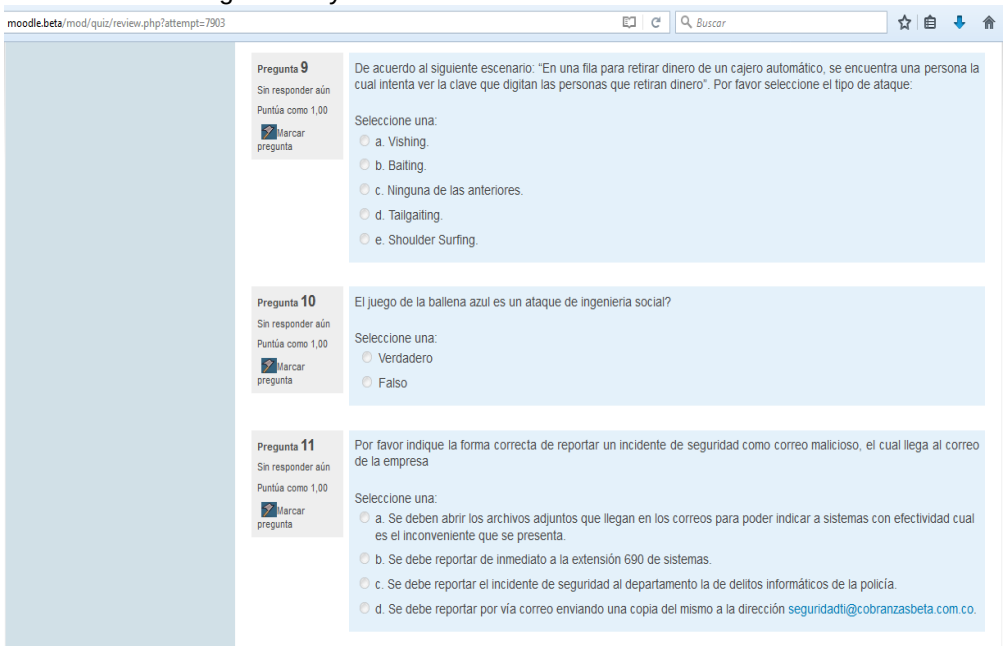
Fuente: Diseñadores del proyecto.

Ilustración 28. Preguntas 7 y 8 fase 3 Moodle



Fuente: Diseñadores del proyecto.

Ilustración 29. Preguntas 9 y 10 fase 3 Moodle



Fuente: Diseñadores del proyecto.

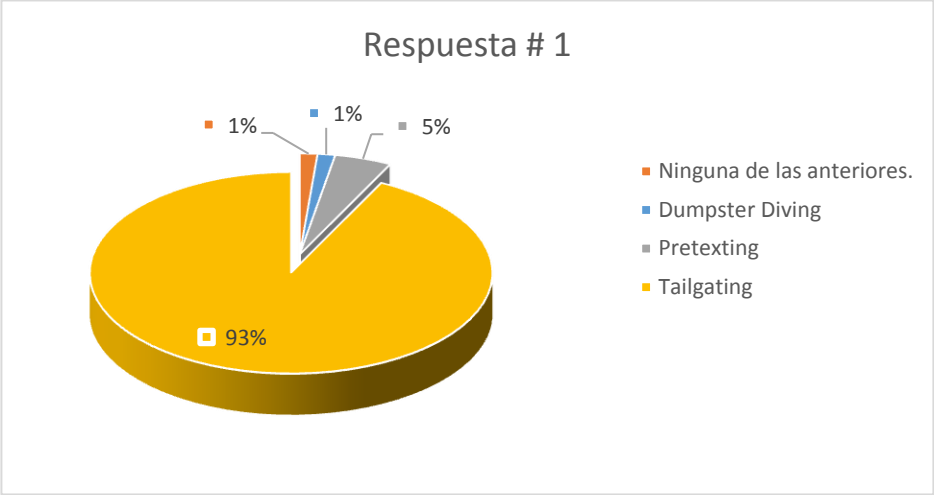
9.2 ANÁLISIS ENCUESTA DE CONOCIMIENTO SOBRE INGENIERÍA SOCIAL - FASE 3

Para determinar si las capacitaciones impartidas al personal de Promociones y Cobranzas Beta han sido efectivas y han llegado a los trabajadores; se realiza una segunda encuesta para determinar el grado de conocimiento adquirido por el personal de Promociones y Cobranzas Beta acerca de la ingeniería social; por lo cual se utilizó la herramienta Moodle que permite realizar seguimiento a cada uno de los participantes, se contó con la participaron de 284 personas de 463 personas que recibieron la capacitación; con respecto a la encuesta inicial se presentó un aumento de participación del 40% de los empleados, lo cual fue significativo ya que en la primera encuesta tan solo participaron 98 personas.

9.2.1 Pregunta 1. De acuerdo al siguiente escenario: "se detecta que una persona ingresa sin registrarse en la recepción de su conjunto residencial, su táctica fue la entrega de un domicilio en un apartamento desocupado", por favor seleccione el tipo de ataque"

9.2.1.1 Análisis respuestas pregunta 1. La pregunta busca evaluar los conocimientos adquiridos en la capacitación de ingeniería social, ya que como se apreció en el sondeo realizado en la primera fase del proyecto la técnica de tailgaiting era desconocida casi por completo, en esta ocasión se presenta un caso en donde el empleado debe deducir que técnica se está utilizando, de modo que se evalúa el conocimiento de los términos de ingeniería social y la capacidad para identificar cada una de ellas; en la Gráfica 8. Pregunta 1 fase 3, se observa que el 93% de las personas encuestadas respondieron correctamente la pregunta, identificando que la técnica de ataque que se representaba era tailgaiting, lo cual demuestra que las capacitaciones realizadas son efectivas; un 7% no identificó el tipo de ataque, lo cual demuestra que es necesario dar una continuidad en capacitaciones de este tipo y realizar campañas de recordación periódicamente buscando disminuir la brecha de seguridad.

Gráfica 8. Pregunta 1 fase 3

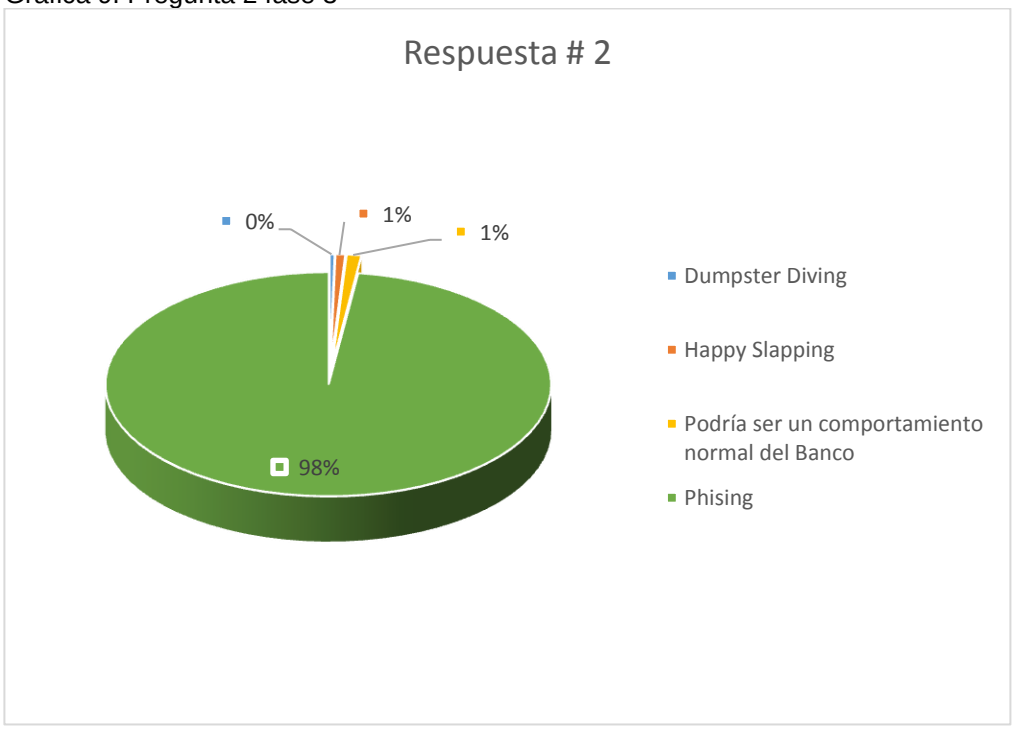


Fuente: Diseñadores del proyecto.

9.2.2 Pregunta 2. De acuerdo al siguiente escenario: "llega a su correo electrónico publicidad del banco, la cual le incita a participar en una promoción en donde se incentiva a usar las tarjetas de crédito. Para motivar a los clientes se promociona la rifa de un automóvil, en donde usted debe realizar un registro a esta página de internet (http://www.davivienda.com)", por favor seleccione el tipo de ataque.

9.2.2.1 Análisis respuestas pregunta 2. La pregunta busca evaluar los conocimientos adquiridos en la capacitación de ingeniería social, aunque la técnica de phishing es de las más conocidas, en el sondeo de la primera fase el 27% de las personas la conocían, en esta ocasión se presenta un caso en donde el empleado debe deducir que técnica se está utilizando, de modo que se evalúa el conocimiento de los términos de ingeniería social y la capacidad para identificar cada una de ellas., se observa en la gráfica de la Gráfica 9. Pregunta 2 fase 3, que el 98% de los encuestados identificaron correctamente que la técnica utilizada fue el phishing, se realiza una retroalimentación a algunos de los empleados preguntando por qué creían que se trataba de un ataque de phising y no de un comportamiento normal del banco, la gran mayoría argumento que las páginas de los bancos deben contar con certificados de seguridad, la dirección de la página al no tener https no les generaba confianza.

Gráfica 9. Pregunta 2 fase 3



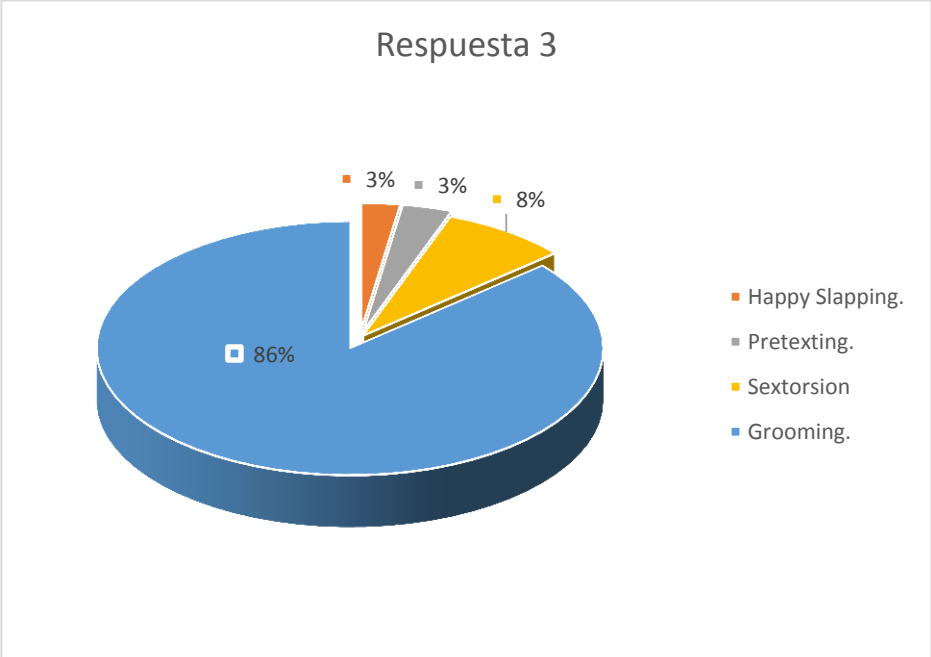
Fuente: Diseñadores del proyecto.

9.2.3 Pregunta 3. De acuerdo al siguiente escenario: “Por medio de Facebook su hijo recibe una invitación de un niño, argumentando que estudian en el mismo colegio. Por medio de chat el niño inicia un juego, donde cada vez que pierda un reto se debe quitar una prenda". Por favor seleccione el tipo de ataque:

9.2.3.1 Análisis respuestas pregunta 3. La pregunta busca evaluar el conocimiento adquirido en la capacitación de ingeniería social, al mismo tiempo que mide el grado de confianza que se tiene en la red social Facebook. La Gráfica 10. Pregunta 3 fase 3, muestra que el 86% de las personas encuestadas seleccionaron correctamente la respuesta, el 14% restante no identifico el ataque confundiéndolo con tipos de ciberbullying.

Durante las capacitaciones se decidió incluir el tema del ciberbullying por solicitud de los empleados quienes querían conocer sobre estos tipos de ataques, los cuales tienen un grado de ingeniería social y es de vital importancia el aprender a identificarlos y a contrarrestarlos ya que es un tema que afecta directamente a menores de edad en la mayoría de casos.

Gráfica 10. Pregunta 3 fase 3

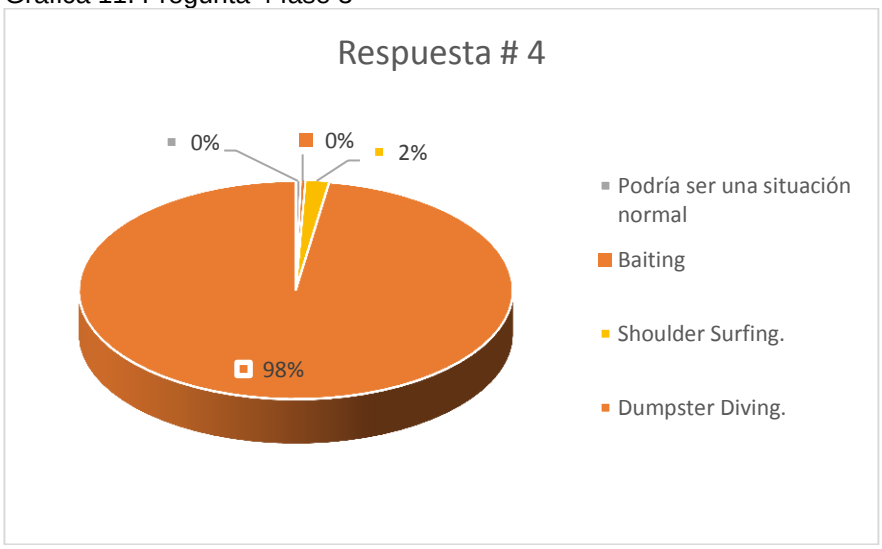


Fuente: Diseñadores del proyecto.

9.2.4 Pregunta 4. De acuerdo al siguiente escenario: "por medio de cámaras de seguridad se evidencia que las personas encargadas del aseo seleccionan papales de la basura". Por favor seleccione el tipo de ataque:

9.2.4.1 Análisis respuestas pregunta 4. La pregunta busca identificar el grado de conocimiento adquirido durante las capacitaciones de ingeniería social. La Gráfica 11. Pregunta 4 Fase 3, muestra que el 98% de las personas encuestadas reconocen un ataque de dumpster diving, los cuales son muy comunes en ambientes empresariales sin descartar a los hogares en donde también las personas pueden llegar a ser afectadas; este es uno de los ataques básicos para empezar a crear estrategias más planificadas de ingeniería social; durante las capacitaciones se indicó las repercusiones que puede tener este tipo de ataques si no se tiene un debido proceso de destrucción de la basura que puede tener información comprometedora, el 2% consideran que es una situación normal, y deberían ser retroalimentados.

Gráfica 11. Pregunta 4 fase 3

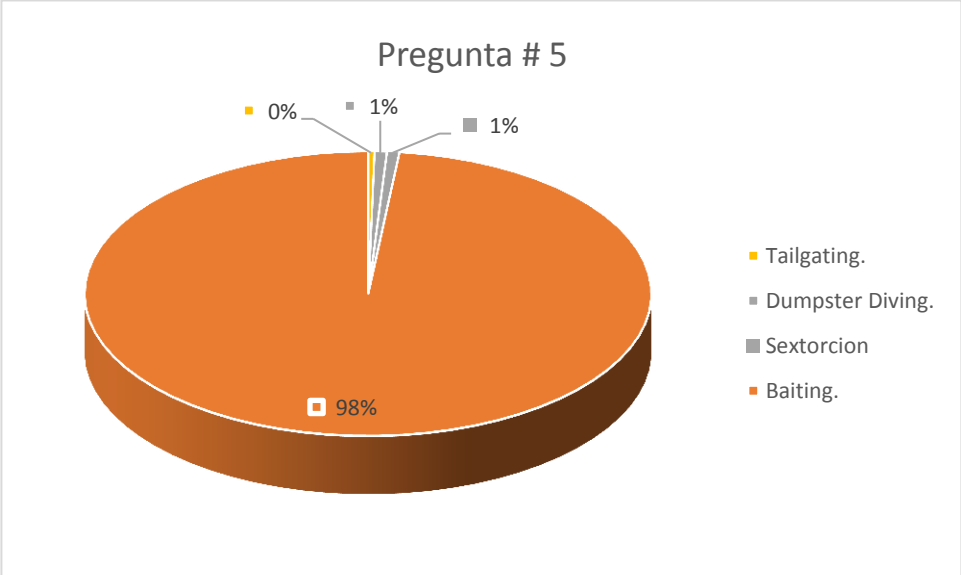


Fuente: Diseñadores del proyecto.

9.2.5 Pregunta 5. De acuerdo al siguiente escenario: “Usted se encuentra en la calle una memoria usb, posterior la conecta al equipo y encuentra que su contenido son archivos de música. Al abrir uno de estos archivos paralelamente se propaga la infección de un virus y un keylogger”. Por favor seleccione el tipo de ataque (un keylogger es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado).

9.2.5.1 Análisis respuestas pregunta 5. La pregunta busca identificar el grado de conocimiento adquirido durante las capacitaciones de ingeniería social. Por medio de la Gráfica 12. Pregunta 5 Fase 3, se puede ver que el 98% de las personas identificó correctamente el ataque, siendo este uno de los ataques en el que se hizo énfasis ya que es comúnmente utilizado y por lo general las personas no son conscientes de que están siendo atacados ya que este tipo de software trabaja bajo el sistema operativo y no es perceptible fácilmente.

Gráfica 12. Pregunta 5 fase 3

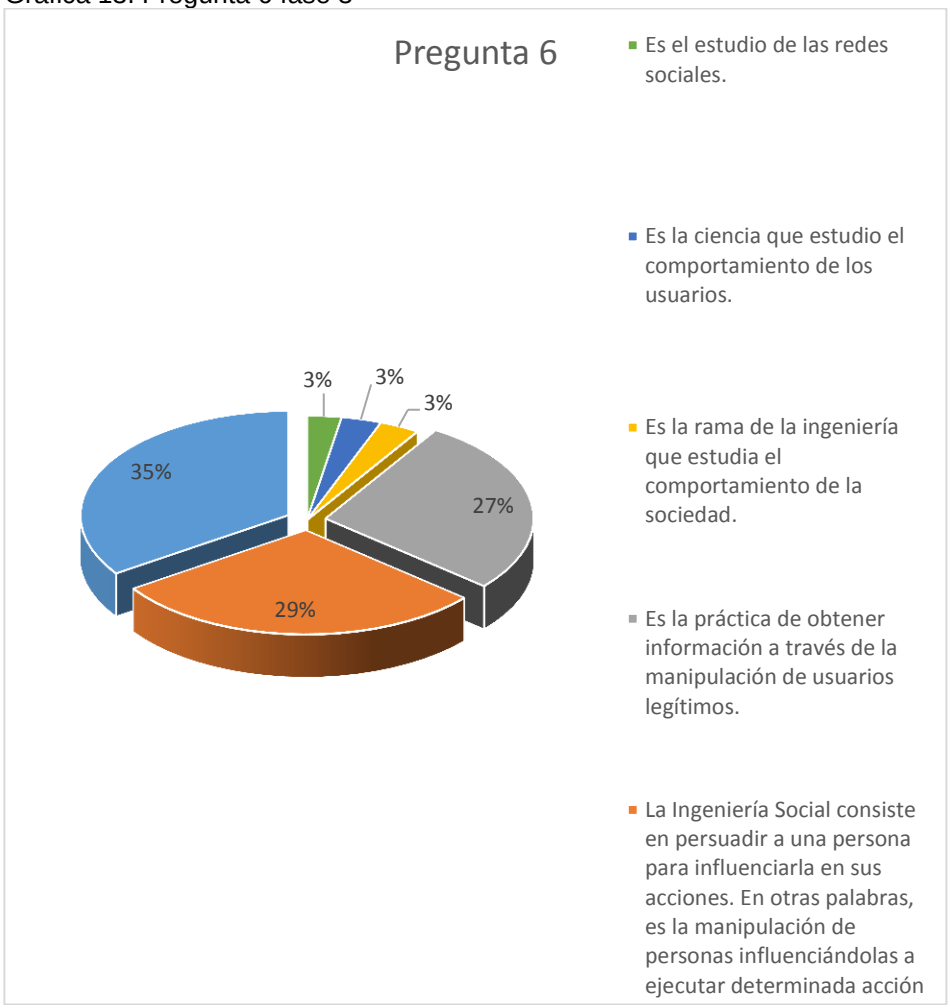


Fuente: Diseñadores del proyecto.

9.2.6 Pregunta 6. ¿Qué es ingeniería social? Seleccione las definiciones que crea correctas.

9.2.6.1 Análisis respuestas pregunta 6. La pregunta busca identificar el grado de conocimiento adquirido durante las capacitaciones de ingeniería social; debido a que durante el muestreo realizado en la primera fase solamente el 58% de los encuestados tenía claro el concepto de ingeniería social. Por medio de la siguiente gráfica podemos ver que las opciones seleccionadas fueron las correctas sumando un 91%; esto demuestra que los empleados tienen claro el concepto de ingeniería social por otro lado tenemos un 9% que seleccionó respuestas incorrectas siendo este un rango importante el cual debe ser mitigado en próximas capacitaciones, en la Gráfica 13. Pregunta 6 fase 3, se puede evidenciar los resultados descritos.

Gráfica 13. Pregunta 6 fase 3



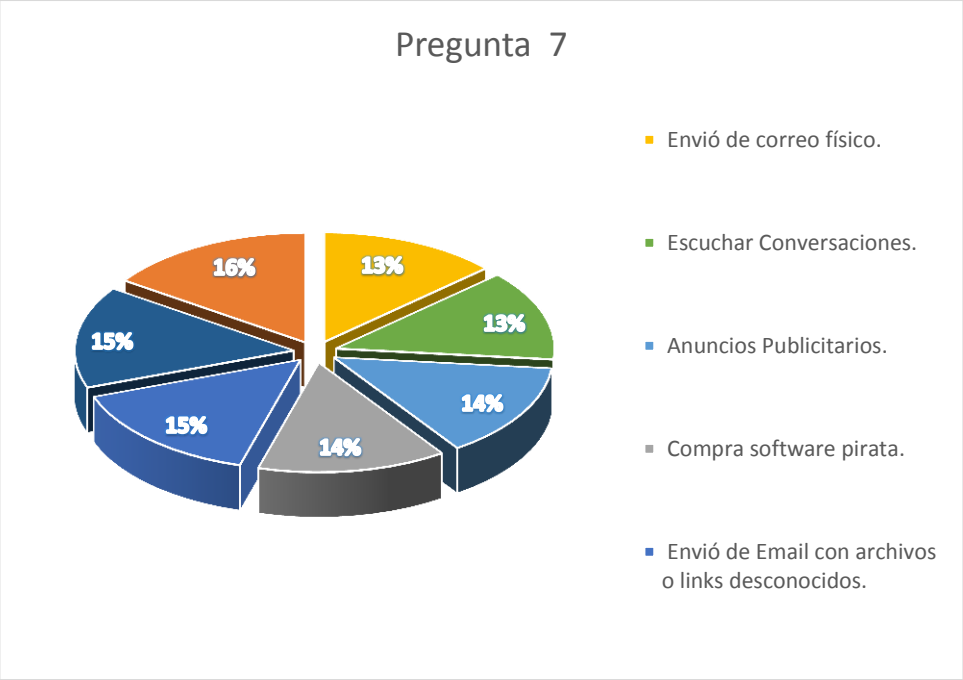
Fuente: Diseñadores del proyecto.

9.2.7 Pregunta 7. ¿En cuál o cuáles de las siguientes opciones cree usted que podría usarse la ingeniería social? Seleccione las opciones que crea correctas.

9.2.7.1 Análisis respuestas pregunta 7. La pregunta busca identificar el grado de conciencia que los empleados tienen sobre los alcances que tiene la ingeniería social; ya que en el sondeo realizado en la primera fase tres técnicas ocuparon el 69% de la torta, dejando al resto de técnicas olvidadas; la Gráfica 14. Pregunta 7 fase 3, nos muestra que las respuestas fueron equilibradas siendo las opciones seleccionadas más bajas, los ataques de envió de correo físico y escuchar conversaciones; esta tendencia se presenta debido a que las personas no son conscientes de que los ataques se presentan en cualquier sitio, con frecuencia en sitios donde las personas bajan la guardia, por ejemplo cafés, restaurantes y fiestas entre otras, por la parte, de los correos físicos las personas no

comprendían como podían ser atacados por medio de publicidad, cartas, notificaciones entre otros medios esto debido a la tendencia a pensar que los ataques siempre provienen desde medios informáticos o tecnológicos; gracias a las capacitaciones esta concepción cambio lo cual podemos ver reflejado al comparar la tendencia de las encuestas.

Gráfica 14. Pregunta 7 fase 3

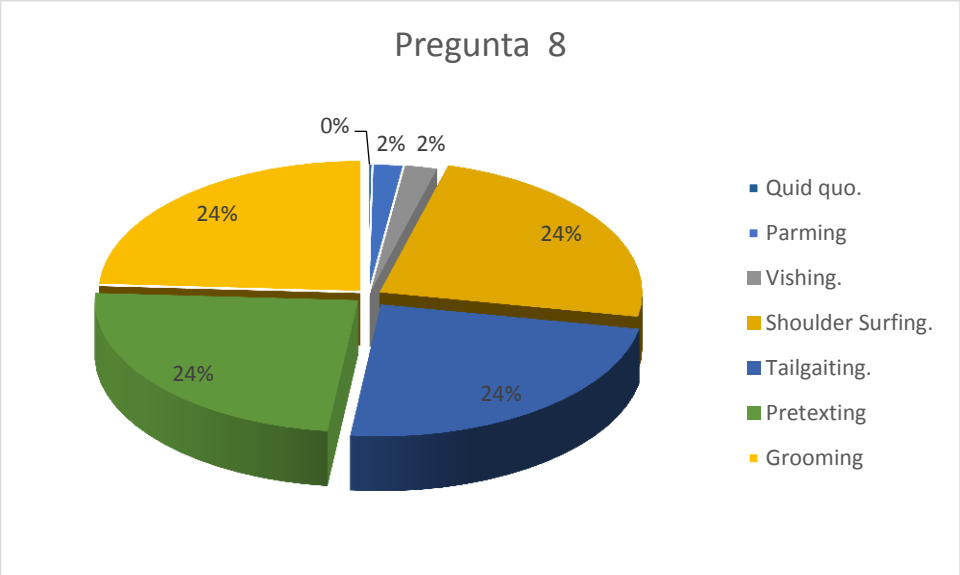


Fuente: Diseñadores del proyecto.

9.2.8 Pregunta 8. Indique cuales de las siguientes técnicas de ingeniería social conoce

9.2.8.1 Análisis respuestas pregunta 8. La pregunta busca identificar cuáles fueron las técnicas de ingeniería social que más causaron impacto y que se tienen más presentes. La Gráfica 15. Pregunta 8 fase 3, muestra que las técnicas de ingeniería social que generaron más recordación son shoulder surfing, tailgaiting, grooming y pretexting cada una con un 24% de la torta; estas técnicas fueron las más recordadas ya que al explicarlas los empleados recordaban que habían escuchado sobre ellas pero no tenían idea de que se trataban de ataques de esta índole, al igual que no conocía cómo protegerse de ellas ni cómo prevenirlos; gracias a la capacitación impartida los empleados adquirieron las competencias necesarias para identificar las técnicas y transmitir este conocimiento a las personas allegadas a ellas.

Gráfica 15. Pregunta 8 fase 3

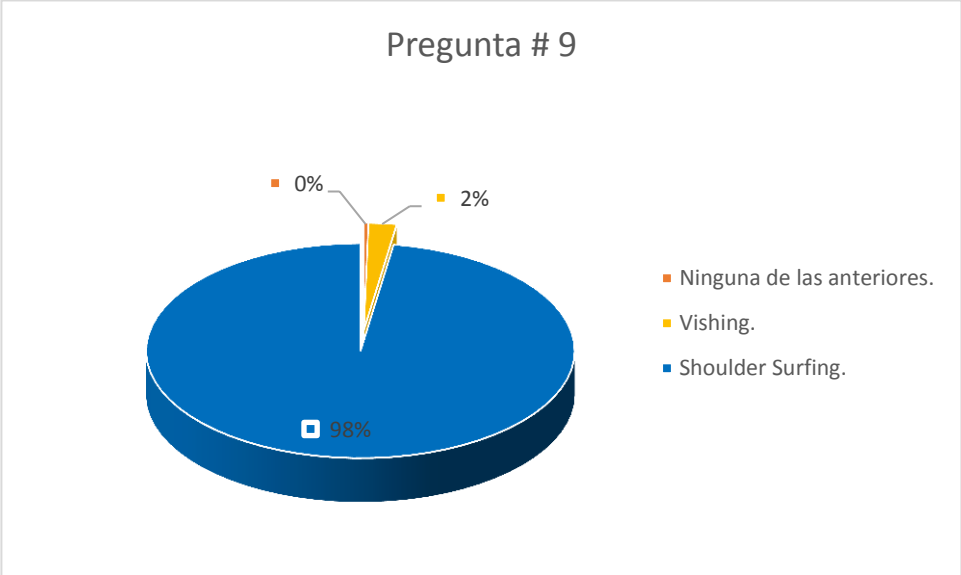


Fuente: Diseñadores del proyecto.

9.2.9 Pregunta 9. De acuerdo al siguiente escenario: “en una fila para retirar dinero de un cajero automático, se encuentra una persona la cual intenta ver la clave que digitan las personas que retiran dinero”. Por favor seleccione el tipo de ataque:

9.2.9.1 Análisis respuestas pregunta 9. La pregunta busca evaluar los conocimientos adquiridos en la capacitación de ingeniería social. La Gráfica 16. Pregunta 9 Fase 3, muestra que el 97% de las personas encuestadas son capaces de reconocer un ataque de shoulder surfing, durante las capacitaciones se hizo énfasis en esta técnica ya que es muy utilizada en cajeros automáticos, sitios públicos donde se consulta información en correo, portales bancarios o cualquier aplicativo que utilice usuario y contraseña y que a su vez sea interesante para un atacante.

Gráfica 16. Pregunta 9 Fase 3

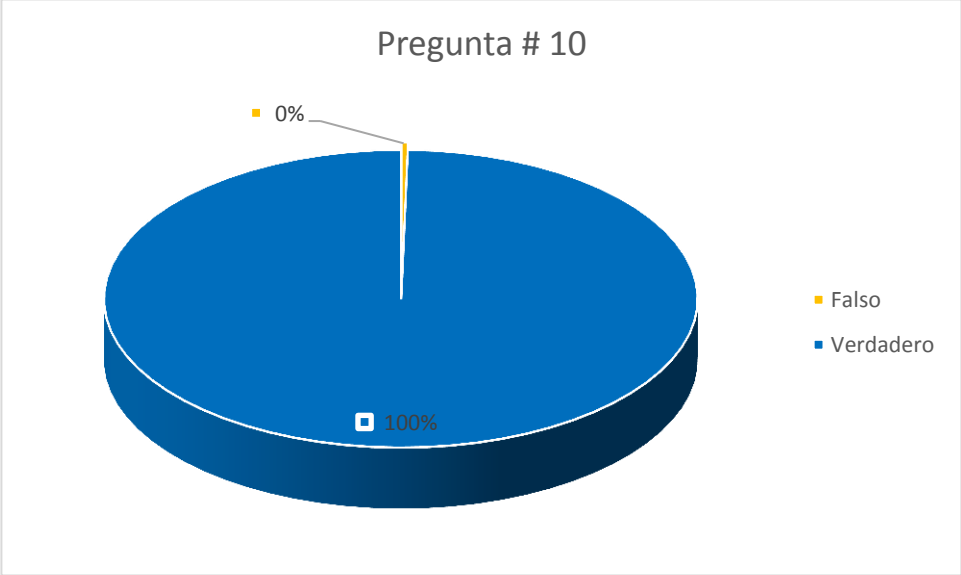


Fuente: Diseñadores del proyecto.

9.2.10 Pregunta 10. ¿El juego de la ballena azul es un ataque de ingeniería social?

9.2.10.1 Análisis respuestas pregunta 10. La pregunta busca evaluar el grado de análisis que realizan las personas ante nuevas técnicas, en este caso el juego de la ballena azul, aunque no es una técnica de ingeniería social si se basa en varias técnicas para lograr su cometido. La Gráfica 17. Pregunta 10 fase 3, muestra que el 100% de las personas contesto que el juego de la ballena azul es una táctica de ingeniería social; esta pregunta se realiza buscando determinar el grado de análisis que tienen los colaboradores sobre eventos que suceden a su alrededor, se determinó que el juego de la ballena azul es un ataque de ingeniería social ya que existe manipulación de individuos.

Gráfica 17. Pregunta 10 fase3



Fuente: Diseñadores del proyecto.

9.2.11 Pregunta 11. Por favor indique la forma correcta de reportar un incidente de seguridad como correo malicioso, el cual llega al correo de la empresa.

9.2.11.1 Análisis respuestas pregunta 11. La pregunta tiene como objetivo determinar la claridad presente en el proceso de reporte de incidentes dentro de la empresa. La Gráfica 18. Pregunta 11 fase 3, permite ver que el 98% de las personas encuestadas tienen claro el proceso de reporte en caso de detección de correo malicioso, esta política se implementó luego de realizar las pruebas de ingeniería social de la primera fase, donde se evidencio que los empleados después de la capacitación empezaron a reportar incidentes de seguridad los cuales antes se pasaban por alto, al recibir estas alertas de seguridad se evidencio que no se tenía una política clara para el reporte de incidentes de seguridad y se creó la política difundiéndola por el área de OYM (Organización y Métodos) quienes son los encargados de generar las políticas y difundirlas a la empresa.

Gráfica 18. Pregunta 11 fase 3

Fuente: Diseñadores del proyecto.

9.3 DEFINICIÓN PRUEBAS INGENIERÍA SOCIAL FASE 3.

La siguiente lista contiene los objetivos seleccionados de acuerdo a características específicas y de acuerdo a los resultados obtenidos en las pruebas realizadas en la fase I.

9.3.1 Phishing.

9.3.1.1 Vulnerabilidad. Usuarios que confían en correos publicitarios, de dudosa procedencia.

9.3.1.2 Objetivo. Por medio de la herramienta Set Tool Kit (SET) se clonará la página (https://cobranzasbeta.facebook.com) de workplace de Promociones y Cobranzas Beta la cual es usada como herramienta de red social interna, tipo Facebook; por medio de correos masivos se invitará a las personas a interactuar con la página dando clic a un enlace el cual los llevará a la página falsa.

9.3.1.3 Descripción usuarios objetivo. Los objetivos seleccionados son todos los empleados de la empresa, ya que la página a clonar está autorizada por la gerencia para todos los trabajadores, el objetivo es evaluar si los empleados han adquirido la habito de revisar los links de los correos antes de acceder a ellos. En el cuadro 35. Objetivos phishing, se menciona el nombre del área a realizar la prueba, el responsable de esta y la cantidad de personas a quienes se enviará el correo

Cuadro 35 Objetivos phishing

Nombre del área	**Responsable**	**Cantidad de personas**
Beta Nacional	Gerente General	463

Fuente: el autor.

9.3.2 Baiting.

9.3.2.1 Vulnerabilidad. Confianza en medios de almacenamiento externos (Pen Drives) de procedencias no verificadas

9.3.2.2 Objetivo. Este ataque se realizará a personas dentro de la compañía que tienen habilitados puertos USB; para la fase 3 se enviara a cada regional una memoria USB con videos alusivos a la seguridad en el trabajo, dentro de los videos que se enviaran se encuentra un autoejecutable el cual se activa cuando se reproducen los videos.

9.3.2.3 Descripción usuarios objetivo. Los objetivos seleccionados son los directores de las 17 sucursales los cuales tienen habilitados los puertos USB. En el Cuadro 36. Áreas objetivas baiting, se detalla el cargo de la persona objetivo y la dirección IP del equipo asignado.

Cuadro 36. Áreas objetivas baiting

Cargo	**Responsable**	**Cantidad de Personas**	**Dirección IP**
Directores regionales	Gerente	17	172.10.X.1

Fuente: Diseñadores del proyecto.

9.3.3 Pretexting.

9.3.3.1 Vulnerabilidad. Usuarios, que por su buena fe de ayudar confían en personas externas o internas, quienes los manipulan con el fin de obtener información confidencial.

9.3.3.2 Objetivo. Se busca realizar un ataque a cada regional dirigido a los auxiliares operativos y auxiliares de sistemas.

9.3.3.3 Descripción usuarios objetivo. Los objetivos seleccionados son usuarios y áreas que tienen acceso a llamadas telefónicas desde el exterior y que cuentan con permisos de usuarios en aplicaciones importantes tales como correo, dominio y generador de Tickets GLPI.

- 5 llamadas a Auxiliares Operativos.
- 5 llamadas a Auxiliares de Sistemas Bogotá.

En el Cuadro 37. Personal objetivo de pretexting se especifica el cargo y segmentos IP de los auxiliares operativos objetivo; en el Cuadro 38. Áreas objetivo de pretexting se menciona el área, responsable e IP para las llamadas que se realizaran a el Área de sistemas.

Cuadro 37. Personal objetivo de pretexting

Cargo	**IP**
Auxiliares operativos	172.10.X.2

Fuente: Diseñadores del proyecto.

Cuadro 38. Áreas objetivo de pretexting

Nombre del Área	**Responsable**	**Cantidad de Personas**
Área sistemas	Auxiliar sistemas	172.10.110.X

Fuente: Diseñadores del proyecto.

9.3.4 Dumpster diving.

9.3.4.1 Vulnerabilidad. Descuido de documentos con información importante o sensible, hojas en impresoras o botes de basura.

9.3.4.2 Objetivo. Recolectar hojas dejadas en impresoras, lugares de papel reciclable y papeleras de basura; con estos documentos se busca posible información valiosa.

9.3.4.3 Descripción usuarios objetivo. Los objetivos seleccionados son todas las áreas que cumplen con la vulnerabilidad. En el Cuadro 39. Áreas objetivo dumpster diving se especifica el área responsable y la cantidad de personas afectadas por esta prueba.

Cuadro 39. Áreas objetivo dumpster diving

Nombre del área	**Responsable**	**Cantidad de Personas**
Sede Bogotá	N/A	200

Fuente: Diseñadores del proyecto.

9.3.5 Shoulder surfing.

9.3.5.1 Vulnerabilidad. Por falta de recordación algunos empleados colocan su clave de red escrita en un papel visible o permiten ver su clave de red fácilmente al digitarla, también aplican los usuarios que dejan sin bloquear las pantallas permitiendo ver la información contenida en los aplicativos abiertos.

9.3.5.2 Objetivo. Obtener usuarios y contraseñas de red; la metodología usada será dar rondas por el edificio en busca de personas que están tecleando usuarios y contraseñas, también se verificaran los papeles pegados en los computadores en busca de información confidencial.

9.3.5.3 Descripción usuarios objetivo. Los objetivos de este ataque son todas las personas que por descuido dejan sus contraseñas visibles al teclearlas, El Cuadro

40. Objetivos shoulder surfing se menciona la sede, cargos, IP, vulnerabilidades y objetivos para la prueba

Cuadro 40. Objetivos shoulder surfing

Nombre	Cargo	IP	Vulnerabilidad	Objetivo
Sede Bogotá	Todos	N/A	Pantallas sin bloqueo, claves predecibles y contraseñas pegadas en el escritorio.	Acceso a equipo sin autorización del funcionario.

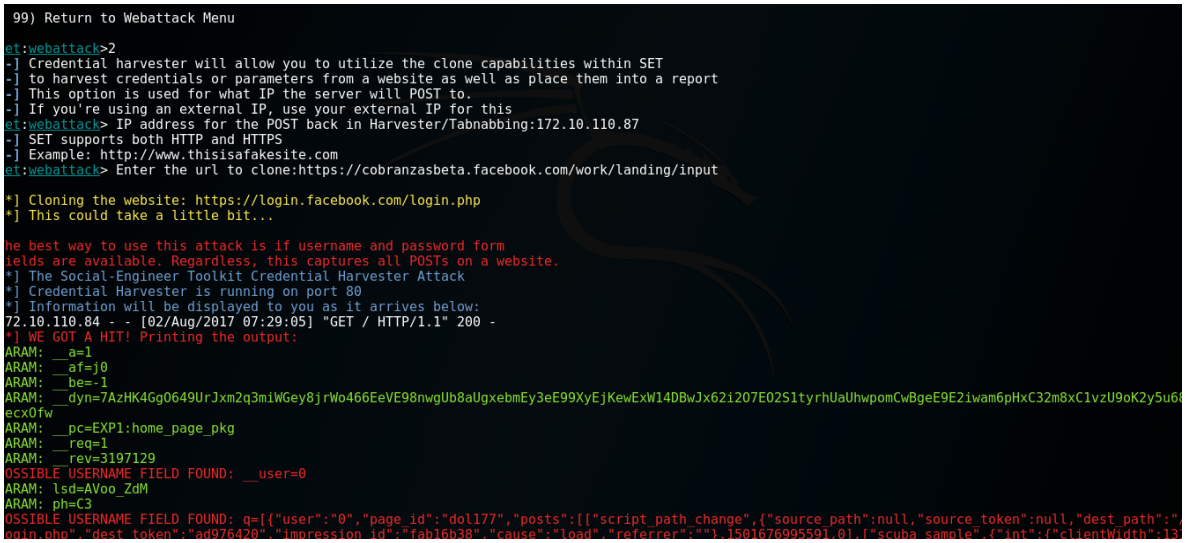
Fuente: Diseñadores del proyecto.

9.4 ANÁLISIS PRUEBAS DE INGENIERÍA SOCIAL - FASE 3

9.4.1 Phishing. Por medio de la herramienta Set Tool Kit (SET) se clonó la página (https://cobranzasbeta.facebook.com) de workplace de Promociones y Cobranzas Beta la cual es usada como herramienta de red social interna, tipo Facebook; por medio de correos masivos se invitó a las personas a interactuar con la página dando clic a un enlace a la página falsa. El resultado de este ataque fue aceptable ya que de 463 correos enviados 36 personas dieron clic en el enlace lo cual quiere decir que el 7% de los trabajadores fueron víctimas de este ataque.

9.4.1.1 Ejemplo de ataque de phishing mediante SET. En la Ilustración 30. Herramienta SET clonación de sitio web, se muestra como está configurada la herramienta Set Tool Kit para recibir la información del ataque, también se muestra cómo se incluye la URL que se desea.

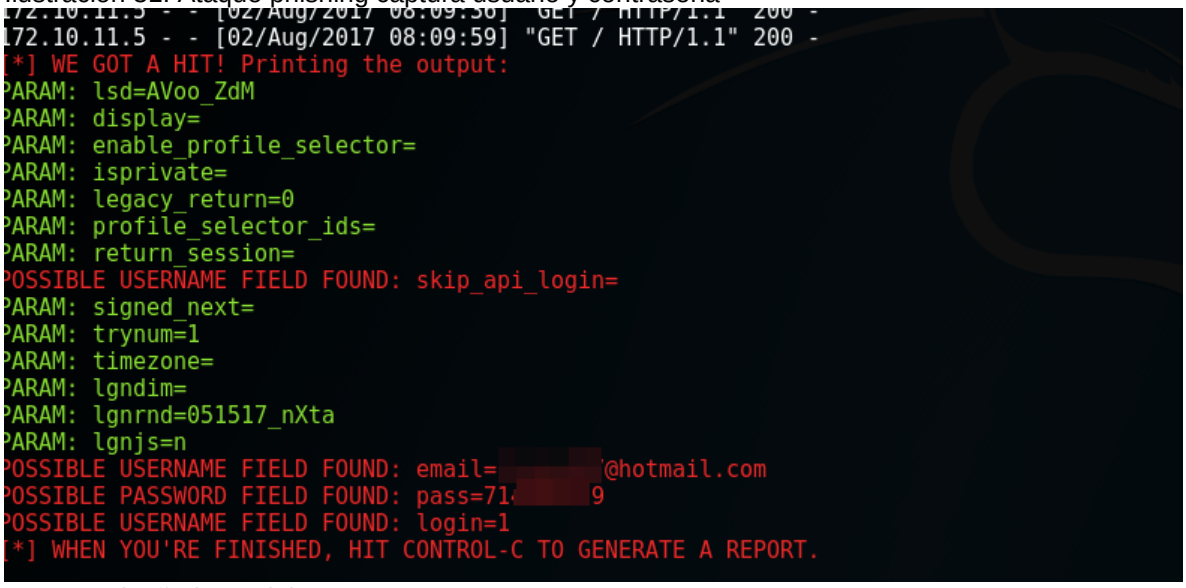
Ilustración 30. Herramienta SET clonación de sitio web



Fuente: Diseñadores del proyecto.

En la Ilustración 31. Ataque phishing captura usuario y contraseña, se muestra como se ha capturado información mediante el ataque programado de phishing con la herramienta SET.

Ilustración 31. Ataque phishing captura usuario y contraseña



Fuente: Diseñadores del proyecto.

9.4.1.2 Aspectos a resaltar.

- Los trabajadores que descubrieron que el correo que se envió promocionando la interacción con la página workplace era falso reportaron correctamente el incidente al área de sistemas.
- Respecto a los primeros ataques de phishing se redujo considerablemente las personas afectadas pasando de un 60% a un 7%.
- Se creó un video institucional el cual cubre todos los temas que se vieron en el plan de concientización, este video tiene la finalidad de realizar una capacitación rápida y efectiva a empleados nuevos para los cuales es un requisito ver el video y pasar una evaluación sobre ingeniería social, la Ilustración 24. muestra varios pantallazos del video.
- Promociones y Cobranzas Beta tomo la decisión de realizar capacitaciones cada 6 meses con el fin de afianzar los conocimientos adquiridos y adicionar nuevos conceptos y técnicas de ataques.

9.3.2 Baiting. Este ataque se realizó a personas dentro de la compañía que tienen habilitados puertos USB y unidades de CD; para la fase 3 se envió a cada regional una memoria USB con videos alusivos a la seguridad en el trabajo, dentro de los videos enviados se encontraba un autoejecutable el cual se activaría cuando se reprodujeran los videos; gracias a las recomendaciones que se realizaron ahora ningún usuario tiene permisos de administrador, debido a esta política el autoejecutable no pudo realizar cambios en el sistema lo cual ocasiono que no fuera posible tomar control remoto computadores en la empresa; de las 17 regionales a las cuales se les enviaron las USB tres (3) se comunicaron con la sede principal en Bogotá y confirmaron la autenticidad de las USB; esto evidencia la necesidad de dar continuidad al plan de capacitación y la necesidad de reforzar más los conocimientos del personal referente a la temática hasta lograr que sea un hábito confirmar la autenticidad de información que llegue a la empresa en medios magnéticos los cuales representen un posible riesgo informático.

También se creó un grupo de Spark (openfire chat) por el cual la información fluye rápidamente y se alerta a las regionales de posibles ataques.

9.3.2.1 Aspectos a resaltar.

- Reporte de algunas sedes sobre la llegada de medios magnéticos.
- Aplicación de políticas desde dominio garantizando la no ejecución de programas.
- Apoyo de las regionales avisando de la llegada de USB con origen desconocido.

9.3.2.2 Aspectos a mejorar.

- Reforzar capacitación a empleados en las técnicas de ataques de ingeniería social.
- Minimizar los equipos que tienen permisos de USB y cd basándose en las cartas descriptivas de los cargos con lo cual se podrá determinar si necesita o no permisos para USB y CD.

9.3.3 Dumpster diving. En la actualidad la empresa cuenta con una máquina trituradora de papel por cada impresora como se puede apreciar en la Ilustración 50, las papeleras de basura fueron retiradas de todos los puestos y en su lugar se ubicaron estratégicamente canecas de reciclaje por colores (ver Ilustración 33. Canecas reciclables de colores) donde los trabajadores deben depositar los residuos según capacitación dictada, las impresoras no usan papel reciclable que contenga información relevante de clientes ni que incluya información financiera, estas hojas son destruidas inmediatamente en las picadoras de papel, es poca y sin importancia la información que se encuentra en las bandejas de papel reciclado de las impresoras.

9.3.3.1 Aspectos a resaltar.

- Adopción de políticas propuestas en el plan de concientización.
- Compromiso de los trabajadores en el reciclaje de basuras y en la catalogación de la información.
- Compromiso de la empresa con el medio ambiente al realizar un adecuado manejo de basuras.

En la Ilustración 32. Picadoras de papel, se aprecian las picadoras de papel adquiridas por la compañía para desechar documentos con información potencialmente sensible.

Ilustración 32. Picadoras de papel

Fuente: Diseñadores del proyecto.

En la Ilustración 33. Canecas reciclables de colores, se aprecian los recipientes de basuras para el control de reciclaje.

Ilustración 33. Canecas reciclables de colores

Fuente: Diseñadores del proyecto.

9.3.3.2 Aspectos a mejorar.

- Seguir capacitando a personal nuevo en la empresa en la importancia de clasificar correctamente la información.

- Realizar una clasificación formal de la información de toda la empresa.
- Implementar picadoras de papel en el resto de las regionales.

9.3.4 Pretexting. Inicialmente se buscó realizar un ataque a cada regional dirigido a los auxiliares operativos y administrativos de cada sede, sin embargo, se realizaron dos llamadas; la primera llamada que se realizó se lanzó desde un teléfono fijo en Bogotá en el cual el atacante buscó ser nuevamente enlazo a una extensión de la sede principal y desde la cual se transfirió a la extensión del auxiliar operativo de la regional; se utilizó el mismo argumento utilizado en la primera fase donde se dijo que era un nuevo auxiliar SENA que ingreso a sistemas; al recibir la posible víctima la llamada, el auxiliar operativo no presto mucha atención a la llamada, pero al momento del atacante solicitar información confidencial a la posible víctima como la contraseña de dominio, este pidió confirmar las credenciales de la llamada recibida con el área de sistemas, al confirmar que la llamada era falsa se dio alerta a sistemas desde donde se alertó a los trabajadores de la empresa sobre posibles ataques de ingeniería social; la segunda llamada que se realizo fue detectada inmediatamente con lo cual no fue posible seguir con los ataques.

Al igual que en la primera fase se encontró una vulnerabilidad en el proceso de entrada y salida de personal de la empresa, la vulnerabilidad consistía en que entre la entrada o salida de personal de la empresa podían pasar más de 15 días sin que el área de sistemas y el área administrativa lo supieran, esto habría una brecha de seguridad en la cual un atacante podría suplantar a una persona recién llegada o recién salida de la empresa, gracias a este hallazgo se tomó por parte de la empresa la decisión de crear un software por el cual se tenga la información actualizada sobre las novedades del personal.

9.3.4.1 Aspectos a resaltar.

- Compromiso de los trabajadores en la puesta en práctica de los conocimientos adquiridos en las capacitaciones dictadas.
- Reporte inmediato al área de sistemas sobre posibles incidentes de seguridad.
- Fluidez en la información enviada a los trabajadores de la empresa.

9.3.4.2 Aspectos a mejorar.

- El caller id de las llamadas que llegan a las regionales transferidas de las extensiones de Bogotá pierde el caller id de origen permitiendo que una llamada desde el exterior de la empresa pase como una llamada interna para los trabajadores de las regionales.
- Al salir o ingresar una persona a la empresa el tiempo que se demora en llegar la información a todas las áreas antes era de 15 días, con el software nuevo

es de máximo 5 días, se debe seguir trabajando hasta que este tiempo se reduzca lo mínimo posible, de este modo se mitigara el riesgo de ataques por suplantación de identidad.

- Iniciativa de la empresa en tomar decisiones radicales con el fin de mitigar los riesgos a los cuales se puede ver expuesta la empresa.
- Compromiso de los trabajadores al aceptar nuevas funciones en pro de la seguridad de la empresa.

9.3.5 Ataques tipo tailgating. Aunque en las recomendaciones que se realizaron se recomendó que las personas siempre tuvieran el carnet de la empresa en un sitio visible algunos trabajadores lo cargan en los bolsillos o en la billetera, al llegar un visitante a las instalaciones en ocasiones se permite que siga a el edificio dándole indicaciones de como llagar a la oficina o área designada.

9.3.5.1 Aspectos a mejorar.

- Realizar refuerzo en la importancia de portar el carnet de empresa en un sitio visible.
- Nunca dejar que personal ajeno a la empresa está circulando sin acompañamiento de un funcionario de la empresa.

9.3.6 Shoulder surfing. Durante las pruebas realizadas en la fase 3 se detectó que el servidor de correo electrónico de la empresa se encuentra publicado en internet, cualquier empleado que cuente con correo electrónico podía acceder a él desde Internet, se tomó la decisión de tomar el servicio de correo corporativo con Microsoft para las cuentas de directores, jefes, coordinadores y supervisores, ya que son los cargos que tendrían la necesidad de consultar el correo desde fuera de la empresa, el correo Zimbra se sigue manejando pero a nivel interno para el resto del personal, con esto se mitigo la fuga de información por medio del correo electrónico y se evitan ataques de fuerza bruta.

9.3.6.1 Aspectos a mejorar.

- Es importante asegurar el servidor de correo Zimbra, aunque a este solamente sea posible el ingreso desde la red interna de la empresa, es importante recordar que muchos de los ataques que se realizan a los servicios se generan internamente.
- Es de considerar la opción de migrar todas las cuentas a office365 ya que la plataforma cuenta con disponibilidad del 99.9% y la seguridad de la misma siempre tiene tecnología de punta.

9.3.6.2 Aspectos a resaltar.

- La empresa fue consciente del riesgo de seguridad que presentaban con el servidor de correo expuesto a internet, razón por la cual decidió hacer una inversión con tal de mitigar el riesgo expuesto.
- Rapidez en la toma de decisiones.

10. BUENAS PRÁCTICAS Y TIPS PARA IDENTIFICAR POSIBLES ATAQUES DE INGENIERÍA SOCIAL EN EL ÁMBITO TECNOLÓGICO, NEUROLINGÜÍSTICO Y PSICOLÓGICO

Es importante conocer el concepto de Programación Neurolingüística ya que este nos atañe directamente; la programación Neurolingüística es más conocida por sus siglas PNL, esta fundamenta sus teorías en la capacidad que tiene una persona de programar acciones o respuestas en otras personas; la palabra "programación" hace referencia a la capacidad de generar un comportamiento deseado en un código informático o como en este caso en personas logrando gestionar un comportamiento ajeno a ellos, el término "neuro" está enlazado con la percepción sensorial que determina nuestro estado de ánimo mientras que la "lingüística" se refiere a comunicación, tanto con lenguaje oral como con el corporal[65] . Dentro de la PNL es importante nombrar una técnica llamada Rapport, término anglosajón el cual no tiene una traducción al español, esta técnica se basa en crear sintonía, logran una sinergia con la persona con la que se está interactuando, tiene como objetivo crear un ambiente agradable y de cooperación mutua.

En el ámbito psicológico la modificación del comportamiento por medio de la intimidación tiene sus inicios en la segunda guerra mundial con las operaciones psicológicas (PSYOP) Psychological Operations o guerra psicológica la cual se centra en aprender todo sobre el objetivo enemigo, gustos, fortalezas, debilidades, aversiones y vulnerabilidades. Ya que una vez se detecté que motiva al objetivo estará listo para comenzar las operaciones psicológicas, mismo comportamiento que se observa cuando se realizan ataques elaborados de pretexting igualmente utilizadas son las fuentes abiertas (OSINT) Open Source Intelligence o inteligencia de fuentes abiertas; Estas fuentes de información hacen referencia a cualquier información desclasificada y públicamente accesible en Internet de forma gratuita; la información más valiosa por lo general se encuentra en la internet profunda fuera del alcance de los motores de búsqueda tradicionales[66].

A continuación, se enmarcan consejos y buenas prácticas de prevención ante ataques de ingeniería social; en primera instancia se debe hacer uso del sentido común, las capacitaciones dictadas, las herramientas de seguridad y apoyarse en el área de seguridad de la empresa al sospechar de posibles ataques.

[65] HACKING CON INGENIERÍA SOCIAL. TÉCNICAS PARA HACKEAR HUMANOS. MUNDO HACKER AÑO DE EDICIÓN2015 EDITORIALRA-MA EDITORIAL

[66] Papeles de inteligencia, ¿Qué son y para qué sirven las fuentes de información OSINT?, actualizado noviembre 2013, disponible en: http://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/

10.1 ¿QUÉ HACER FRENTE A UNA SUPLANTACIÓN DE IDENTIDAD?

Estar alerta siempre al recibir llamadas de desconocidos quienes soliciten información personal; por lo general este tipo de personas cuenta con muchos datos personales y de las empresas; al realizar este tipo de ataques realizan una recopilación de información por (OSINT) Open Source Intelligence o Inteligencia de fuentes abiertas la cual puede durar meses hasta que el atacante detecte una vulnerabilidad y cree un ataque elaborado; los delincuentes informáticos suelen suplantar personal de soporte técnico, proveedores de servicios públicos y privados; estas personas siempre estarán intentando solicitar información de contraseñas, usuarios, números de tarjetas de crédito o cualquier información que genere lucro financiero.

10.1.1 Recomendaciones.

- Siempre que quienes llaman sean aduladores, manejen un tono de voz similar al nuestro, busquen generar mucha empatía, debemos desconfiar ya que podríamos estar ante una técnica de rapport.
- Solicitar y confirmar las credenciales de identificación con las respectivas empresas, ya que por medio de (OSINT) Open Source Intelligence o Inteligencia de fuentes abiertas podrían tener información muy puntual sobre la empresa y sobre nosotros.
- Cuando quienes llaman son repetitivos y reiterativos en aspectos puntuales de la comunicación debemos desconfiar ya que podrían estar utilizando técnicas de PNL o Programación Neurolingüística.
- Lo mejor es analizar cada una de las respuestas que se va a entregar y pensar por un momento si estas podrían ser utilizadas para un mal proceder, es importante la cautela cuando se está conociendo o interactuando con personas nuevas o desconocidas.

10.2 PHISHING.

Al momento de recibir correos electrónicos los cuales incluyan enlaces a otras páginas, correos que soliciten información confidencial o archivos adjuntos es necesario siempre tener plena seguridad de la fuente y confiabilidad del enlace adjunto, especialmente si la cuenta remitente es desconocida; aunque no se debe bajar la guardia con los correos conocidos ya que también pueden ser suplantados; estos ataques también suelen cometerse mediante archivos SMS, se debe validar minuciosamente este tipo de comunicaciones y si se desconfía de su procedencia es preferible borrarlo y solicitar la confirmación del envió, si es necesario se solicitara el reenvió del mismo.

10.2.1 Recomendaciones.

- Nunca se debe entregar información por medio de correo electrónico o por ningún otro medio de comunicación; siempre se debe desconfiar cuando soliciten claves de acceso, usuarios, datos personales o números de tarjeta de crédito.
- Se debe prestar mucha atención a los enlaces que vienen en los correos electrónicos antes de abrirlos es recomendable verificar a donde nos direccionan, esto lo podemos comprobar con situar el cursor del mouse sobre el enlace sin dar clic.
- Es muy común que los correos de phishing traten temas de actualidad o chismes de famosos, acudiendo a la curiosidad humana y de esta forma hacer que caigan en la trampa.
- Desconfiar de cualquier tipo de correo el cual ofrezca ganar dinero fácilmente.
- Desconfiar de archivos adjuntos especialmente si son ejecutables, comprimidos o con extensiones poco frecuente como js, hta y vbs por nombrar algunas, se recomienda borrarlos a menos que se confirme con la fuente el contenido y el propósito del mismo.
- Siempre que se acceda a una página es aconsejable verificar la dirección o escribirla directamente en el navegador, si se accede a entidades bancarias siempre se debe verificar que la página cuente con certificados de seguridad https.
- En lo posible nunca utilice computadores de café internet si debe introducir usuarios, contraseñas o si debe realizar algún tipo de transacción.

10.3 DUMPSTER DIVING.

Al desechar documentos se debe verificar que estos no contengan información sensible como números de cuenta, libretas telefónicas, usuarios, claves, manuales, garantías y bases de datos entre otra información que pueda ser valiosa para un delincuente informático.

10.3.1 Recomendaciones.

- Destruir los documentos que contengan información confidencial cuando no se vallan a utilizar o archivar, es aconsejable utilizar picadoras de papel, en la ausencia de picadoras utilizar tijeras o destruir los documentos con agua u otro tipo de líquidos.
- Se debe verificar que el personal que recoge los desechos sea confiable.
- Nunca desechar unidades usb, discos duros, cd, dvd o cualquier medio magnético sin realizar un borrado seguro de la información con herramientas como Eraser, HDDErase, WipeFile o KillDisk entre algunas otras herramientas del mercado.

10.4 REDES SOCIALES.

Las redes sociales deben ser configuradas con los diferentes niveles de seguridad y privacidad que estas brindan con el fin de no compartir información que pueda ser usada con fines malintencionados en la red.

10.4.1 Recomendaciones.

- Se debe ser muy cuidadoso al publicar información en las redes sociales ya que esta información puede ser utilizada por los delincuentes informáticos en contra nuestra.
- Al ingresar a una red social se debe configurar los niveles de seguridad y privacidad, esto ayudará a compartir información solo con personas cercanas y no quedará como información pública expuesta.
- Se recomienda utilizar una palabra clave entre los miembros de la familia, con esta clave podremos desenmascarar un ataque de suplantación de identidad, adicionalmente es una buena práctica enseñarla a los menores de edad en casa e indicarles que en caso de pérdida soliciten la contraseña secreta.
- En caso de sospechar de un ataque de suplantación de identidad es aconsejable confirmar por medio de otra línea si la persona suplantada está bien o si efectivamente la llamada es legítima.
- En caso de extorsión se aconseja nunca acceder a los chantajes, informar a la línea anti extorción (Resto del País 018000910112 o en Bogotá 5159111 / 9112).

10.5 SOFTWARE MALICIOSO MEDIANTE BAITING

Hay que tener precaución con este tipo de ataque, ya que por medio de esté un ciberdelincuente puede lograr infectar equipos y redes enteras por lo general se utilizan medios extraíbles como usb, dvd, cd o discos externos los cuales están infectados con software malicioso como por ejemplo virus, troyanos, spyware, keylogger, mazar y ramsonware entre otros; al insertar el medio magnético en el dispositivo (pc, portátil, smart phone o tableta).

10.5.1 Recomendaciones.

- Mantener el sistema operativo con las últimas actualizaciones del sistema operativo, de esta forma se protege el software del equipo ante vulnerabilidades descubiertas recientemente.
- Contar con un buen producto antivirus y antimalware, mantenerlo actualizado con las ultimas definiciones lo que ayudará a mitigar el riesgo de contagio.
- No abrir dispositivos desconocidos antes de realizar una revisión exhaustiva con un antivirus y antimalware; esto aplica también para archivos adjuntos en correos electrónicos.
- Evitar navegar por páginas no seguras o con contenido no verificado.

- Generar una copia de seguridad de la información, esta copia se debe almacenar fuera del dispositivo.
- En caso de chantaje para recuperar la información, reporte inmediatamente al comando de acción inmediata (CAI) virtual de la policía www.caivirtual.policia.gov.co
- Se aconseja no utilizar usuarios con permisos de administrador, ya que estos tienen los permisos necesarios para instalar cualquier programa sin necesidad de realizar una verificación de permisos de usuario.
- Se recomienda que los niños que utilizan dispositivos con salida a internet tengan un perfil de usuario restringido y controlado por una herramienta de control parental lo cual protegerá de accesos a contenido potencial mente peligrosa.
- Nunca bajar software de páginas con dudosa reputación las cuales ofrecen programas gratis los cuales son pagos, estos programas suelen estar modificados para abrir puertas traseras e instalar software malicioso sin que el usuario se llegue a dar cuenta; nunca comprar software pirata ya que este podría estar alterado de la misma forma que el software que se descarga de internet.
- Nunca conectarse a redes Wifi desconocidas ya que por medio de estas es posible capturar el tráfico y lanzar ataques a programas instalados en los dispositivos logrando obtener control total de dichos equipos comprometiendo la información almacenada y poniendo en descubierto claves y usuarios.

10.6 SEGUIR PROTOCOLOS DE SEGURIDAD

Es importante crear conciencia entre los empleados y que sean formados sobre cómo detectar potenciales amenazas de seguridad ya que este aspecto es muy importante debido a que el ser humano es el eslabón más débil en la cadena de la seguridad informática.

10.6.1 Recomendaciones.

- Capacitar continuamente a los empleados en la detección de amenazas de seguridad y realizar evaluaciones periódicas.
- Las políticas de seguridad deben ser difundidas, comprendidas y aplicadas por todos los funcionarios de la empresa.
- Es recomendable la realización de pruebas de seguridad periódicos que permitan medir cómo se comportan los funcionarios ante amenazas informáticas; esto es importante ya que las vulnerabilidades que afectan a sistemas operativos o las técnicas de ingeniería social cambian constantemente y de ahí la frase que dice que una empresa nunca está totalmente segura.
- La implementación de un equipo de respuesta frente a incidentes de seguridad informática (CSIRT), el cual está conformado de un grupo de profesionales los

cuales analizan las situaciones y responden con efectividad ante una amenaza informática.

11. CONCLUSIONES

Con la fase 1 luego de realizar la recolección de la información y hacer un reconocimiento de la empresa, se consigue analizar los posibles escenarios en los cuales los empleados de Promociones y Cobranzas Beta S.A podrían ser víctimas de ataques de ingeniería social a partir de la observación de procesos, horarios y cotidianidad en el día a día de los empleados. Una vez analizados los posibles escenarios se realiza una encuesta consiguiendo que el 21% de la población diligenciara la misma y de esta manera contar con un margen de confiabilidad en la encuesta de un 95% según la fórmula de muestreo de Murray y Larry (2005), mediante esta muestra recolectada es posible evidenciar la necesidad de concientización sobre dicha temática; también se realizan pruebas de ingeniería social en donde los resultados obtenidos evidencian la necesidad de ejecución de un plan para informar a los colaboradores de la compañía sobre este método de ciberdelincuencia que amenaza a la población en general.

En la fase 2 se realiza el diseño y ejecución de un plan de concientización, el cual entrega unos óptimos resultados en donde el 68% de la población esperada recibió la capacitación.

Para la Fase 3 una vez entregada la información referente al tema de ingeniería social, a los colaboradores de la compañía, se realiza por segunda oportunidad una nueva encuesta, en donde se evidencia con la misma que ahora los empleados han adquirido un nuevo conocimiento con referente al tema, y a pesar de que existen algunas respuestas no satisfactorias, en su mayoría ya conocen del tema; a su vez también se realizan unas pruebas por segunda vez de ingeniería social, las cuales muestran por su poca efectividad a diferencia de en la primera oportunidad como los empleados se encuentra mejor preparados para hacer frente a esta problemática

Acorde a los resultados expuestos se generó un plan de concientización diseñado específicamente para Promociones y Cobranzas Beta el cual entrego a gran parte del personal un nuevo conocimiento y ayudo a contar con perspicacia para hacer frente a posibles ataques de ingeniería social; a su vez se entregó material a la empresa para que mantengan informados a sus colaboradores y puedan dar continuidad en la concientización, buenas prácticas y tips, que permitirán identificar posibles ataques de ingeniería social en el ámbito tecnológico, neuro lingüístico y psicológico.

En términos generales la firma queda en un nivel más alto de conocimientos frente a la ingeniería social a como se encontraba al iniciar el plan de concientización; durante los 12 meses que duro el proyecto se implementaron políticas dirigidas a mitigar las vulnerabilidades encontradas se realizaron capacitaciones sobre cómo identificar y como repeler ataques de esta índole, con lo cual se generó conciencia en el personal y las competencias necesarias para ser capaces de proteger la empresa, la familia y allegados ante este tipo de ataques.

BIBLIOGRAFÍA

Alegsa, DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA, Latino América, sin fecha de actualización, [en línea], disponible en Internet: http://www.alegsa.com.ar., consultado el 07 de Julio de 2016

AVILÉS GÓMEZ, Manuel, et al. Delitos y delincuentes: cómo son, cómo actúan. San Vicente, España: ECU, 2010. 404 p. ISBN 978–84–9948–151–7.

B: SECURE. “Hackers filtran datos de Harvard, Stanford y Princeton”, octubre 2012. Disponible en internet: http://www.bsecure.com.mx/featured/hackers-filtran-datos-de-harvard-stanford-y-princeton, consultado el 10 de mayo de 2017.

Biblioteca pleyades, operaciones psicológicas de guerra, Latino América, disponible en internet: https://www.bibliotecapleyades.net/sociopolitica/esp_sociopol_mindcon85.htm, consultado el 15 de enero de 2017

Carl Marklund, "Adjusting Facts and Values- Reconciling Politics witch Science: Some Notes on the Rhetorics of Social Engineering in Depression - Era Sweden and USA," Ideas in History 11.2 (2007) 10.

Caruana, Pablo M, "Breves Conceptos sobre la Ingeniería Social", 2001, disponible en internet http://virusattack.xnetwork.com.ar/articulos/VerArticulo.php3?idarticulo=4 , consultado el Domingo, 02 de octubre de 2016.

CHASQUI, junio 2002. Disponible en internet: http://www.redalyc.org/pdf/160/16007810.pdf ISSN 1390-1079. Consultado el Domingo 07 de mayo de 2017

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 23. (28, enero, 1982). “Sobre derechos de autor”. Bogotá, D.C., a 28 de enero de 1982.

Colombia. Congreso de la república. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan Disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1

_____. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4

_____.. Ley Estatutaria 1266 DE 2008: "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". Bogotá, D. C., a 31 de diciembre de 2008.

CPU 2012 al 2014–Revista de Coordinación de Psicología del Uruguay, Relaciones, Uruguay 2009 al 2014 – Publicación semanal sobre psicología

EL ESPECTADOR. “Capturan a 22 'mercenarios' informáticos por millonario robo a Colpensiones"”, 10 de junio 2013, disponible en internet: http://www.elespectador.com/noticias/nacional/cae-red-de-hackers-robo-mas-de-1000-millones-articulo-426933, consultado el 10 de mayo de 2017.

_____. “Capturan a 22 'mercenarios' informáticos por millonario robo a Colpensiones"”, 23 de octubre de 2015, disponible en internet: http://www.elespectador.com/noticias/judicial/capturan-22-mercenarios-informaticos-millonario-robo-co-articulo-594594, consultado el 10 de mayo de 2017.

_____. “Ciberataques a celulares se disparan, según estudio”, 26 de junio de 2013, disponible en internet: http://www.elespectador.com/tecnologia/ciberataques-celulares-se-disparan-segun-estudio-articulo-430140, consultado el 10 de mayo de 2017.

_____. “Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional”, 17 Mar 2015, disponible en internet: http://www.elespectador.com/noticias/educacion/hackean-cuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936, consultado el 09 de mayo de 2017.
El Mundo.es "¿Cuánto puede tardar un 'hacker' en adivinar tu contraseña?", 09/02/2016, disponible en internet:

http://www.elmundo.es/papel/todologia/2016/02/09/56b1fc68268e3e70488b4572.html, consultado el 10 de mayo de 2017

Enter.co, "Bancolombia advirtió por estafa en red usando la marca del banco ", 14 de marzo de 2017, disponible en internet: http://www.enter.co/chips-bits/seguridad/usuarios-bancolombia-tips-para-no-caer-en-el-ataque-de-phishing/, consultado el 17 de mayo de 2017.

Es.ccm.net "El 50% de las empresas víctimas de la ingeniería social", actualizado en mayo 2017, disponible en internet: http://es.ccm.net/faq/7695-el-50-de-las-empresas-victimas-de-la-ingenieria-social, consultado el 17 de mayo de 2017

FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI, junio 2002. Disponible en internet: http://www.redalyc.org/pdf/160/16007810.pdf ISSN 1390-1079. Consultado el Domingo 07 de mayo de 2017

Hadnagy Christopher, “Social Engineering the art of human hacking”, Chapter 1. Editorial Wiley Publishing inc. 2011, p 23-31.

Hansen Dennis, “SAVE Social Vulnerability & Assessment Framework”, Dennis Hansen (ed.) Royal Danish Defence College, febrero 2017, Glosario.

Hipertextual.com, JJ Velasco “Kevin Mitnick, un hacker de leyenda en la Campus Party de Valencia”, 14 julio 2011, Disponible en internet: https://hipertextual.com/2011/07/kevin-mitnick-un-hacker-arrepentido, Consultado el miércoles 25 de mayo de 2017

HSB Noticias.com, "Bancolombia advirtió por estafa en red usando la marca del banco ", jueves, 16 de marzo de 2017, disponible en internet: http://hsbnoticias.com/noticias/tus-finanzas/bancolombia-advirtio-por-estafa-en-red-usando-la-marca-del-b-284930, consultado el 17 de mayo de 2017.

INFORMADOR.MX. “Estudiantes “hackean” calificaciones de su Universidad”, febrero 2009, Disponible en internet: http://www.informador.com.mx/internacional/2009/75916/6/estudiantes-hackean-calificaciones-de-su-universidad.htm , consultado el 07e mayo d e2017

ISO/IEC 13335-1:2004 Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ISO/IEC 27000, Términos y definiciones, 2014, sección 2.

Jenkins, Henry (2006) Convergence Culture, New York University Press, New York

K. Mitnick and W. Simon, The art of deception. Indianapolis: Wiley, 2002.

Kasperski, Seguridad 101: Los tipos de malware, Kasperski Lab, actualizado el 10 de mayo de 2016. Disponible en internet: http://support.kaspersky.com/sp/viruses/general/614, Consultado: miércoles, 03 de Agosto de 2016.

LA TERCERA. “Hackean página web de la Universidad Católica con sitios pornográficos”, marzo 2012. Disponible en internet: http://www.latercera.com/noticia/hackean-pagina-web-de-la-universidad-catolica-con-sitios-pornograficos/, consultado el 10 de mayo de 2017

M. Nohlberg, “Social engineering: understanding, measuring and protecting against attacks”, ph.d. Licenciature, dept. Hum. And inf., univ. Of skövde, Sweden, 2007.

MEDINA, Edgar. Redacción Tecnosfera. Ingeniería social, la razón del éxito de los ladrones digitales, El Tiempo, Bogotá, 1 de julio de 2015. Disponible en internet: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/de-que-se-trata-la-ingenieria-social/16020156, Consulta: lunes, 01 de agosto de 2016.

Merriam-Webster, definición de Ingeniería social, Enter, Editorial triple, sitio web Actualizado: viernes, 30 de septiembre de 2016. Disponible en internet: http://www.merriam-webster.com/dictionary/social+engineering, Consulta: Domingo, 02 de octubre de 2016.

Ministerio de defensa de la Republica de Colombia, "Política de defensa y seguridad", 2015, disponible en internet: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Descargables/espanol/politica_defensa_deguridad2015.pdf, consultado el 18 de mayo de 2017.

_____ Policía Nacional, RESOLUCIÓN 03049 del 24 de agosto de 2012, "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", ARTÍCULO 5. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, definición de Ingeniería social, Enter, Editorial triple, sitio web Actualizado: viernes, 30 de septiembre de 2016. Disponible en internet: http://www.mintic.gov.co/portal/604/w3-article-18800.html, Consulta: Domingo, 02 de octubre de 2016.

Nederlandsch Economisch-Historisch Archief: J.C. van Marken - Biografisch portret bio en Wiki francesa: Émile Cheysson William Howe Tolman (1909):

Panda security ¿Qué es un Ransom ware?, Latino América, disponible en internet: http://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/, consultado el 05 de marzo de 2018

Papeles de inteligencia, ¿Qué son y para qué sirven las fuentes de información OSINT?, actualizado noviembre 2013, disponible en internet: http://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/ consultado el 20 de julio de 2017

Pontiroli Santiago, Kasperski, Ingeniería Social: Hackeando el sistema operativo del ser humano, actualizado el 23 de diciembre de 2013. Disponible en internet: https://blog.kaspersky.com.mx/ingenieria-social-hackeando-el-sistema-operativo-del-ser-humano/1839/ , Consultado el sábado 06 de mayo de 2017.

Programacion-neurolinguistica, Latino América, ,disponible en internet: https://psicologiaymente.net/vida/programacion-neurolinguistica, consultado el 23 de junio de 2017

Promociones y Cobranzas Beta, "Nuestra Empresa", no disponible fecha de publicación, disponible en internet : http://cobranzasbeta.com.co/desarrollo/content/nuestra-empresa, consultado el 28 de junio de 2017.

Psicoterapeutas, ¿Qué es el Rapport?, marzo 10 de 2010, Editado por la Dra. Moya Guirao, disponible en internet: http://psicoterapeutas.eu/rapport/, consultado el 08 de agosto de 2017

Pulzo.com, "Alerta de seguridad informática en Bancolombia ya fue solucionada", 14 de marzo de 2017, disponible, en internet: http://www.pulzo.com/tecnologia/respuesta-bancolombia-campana-phishing/PP228776 , consultado el 17 de mayo de 2017.

RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. “Ingeniería Social, una amenaza informática”, septiembre 2009. Disponible en internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica, Consultado el domingo 07 de mayo de 2017.

Ramos Varón a, Hacking con Ingeniería Social. Técnicas para hackear humanos. Mundo hacker año de edición 2015 editorial ra-ma.

Rodriguez, Ernesto,"Tema: Mestra y Muestreo", 2012, disponible en internet: https://www.uaeh.edu.mx/docencia/P_Presentaciones/tizayuca/gestion_tecnologica/muestraMuestreo.pdf, consultado el jueves, 13 de Julio de 2017.

SANTOS, Guillermo, Ingeniería Social: el hackeo humano (entrevista), Caracol Radio, Bogotá, 31 de agosto de 2011. Disponible en internet: http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html, Consulta: miércoles, 03 de agosto de 2016.

Sin autor. Conozca de qué se trata la 'Ingeniería Social' y tome precauciones, Revista Semana, Publicaciones Semana S.A, Bogotá, 30 de enero de 2014. Disponible en internet: http://www.semana.com/tecnologia/tips/articulo/conozca-que-trata-ingenieria-social-tome-precauciones/373280-3, Consulta: miércoles, 03 de Agosto de 2016.

Social Engineering New York Times: Dr. Tolman Sails on His Mission. David Östlund (2007): The Business Career of the Terminology of Social Engineering 1894-1910

Social-Engineer.org, Marco de referencia de Ingeniería Social, Discusión general, los Hackers, Social Engineer, Inc.2016, consultado el 10 de agosto de 2016.

Symantec, Glosario de Seguridad 101, Latino América, sin fecha de actualización, [en línea], disponible en Internet: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad, consultado el 18 de Agosto de 2016

T. Qin and J. K. Burgoon. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering, Univ. Of Arizona, 2007.

Talamantes, Jeremiah. The Social Engineer's Playbook: A Practical Guide to Pretexting (pp. 4-5). Hexcode Publishing. Edición de Kindle.

Universidad de Nevada, Las Vegas, "Definition of Information Security", 2015, disponible en internet: https://oit.unlv.edu/network-and-security/definition-information-security, consultado el 18 de mayo de 2017.

WeLiveSecurity.com, Noticias, opiniones y análisis de la comunidad de seguridad de ESET, "¡No tan rápido! Esa publicación de Facebook podría no ser lo que parece ", publicado en febrero 3 de 2016, disponible, en internet https://www.welivesecurity.com/la-es/2016/02/03/no-tan-rapido-publicacion-de-facebook/ , consultado el 17 de mayo de 2017

ANEXOS

Anexo A. Acta de reunión 1

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

ACTA DE REUNION No. 01	
Tema: definición de objetivos y necesidades para la ejecución del proyecto de diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa Promociones y Cobranzas Beta S.A.	
Nombre de la reunión: Inicio de actividades del proyecto de diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa Promociones y Cobranzas Beta S.A.	
Fecha de la reunión: 19 de agosto de 2016	
Lugar de la reunión: sala de reuniones sótano sede principal Bogotá, Promociones y cobranzas Beta S.A.	
Asistentes: Ing. Alexander – Director de Sistemas	Ing. Alejandro Torres – ejecutor del proyecto Ing. Danny López – ejecutor del proyecto

Objetivos de la reunión:

- Definir objetivos del proyecto para la empresa Promociones y Cobranzas beta S.A.
- Acordar necesidades por parte de los ejecutores, para la ejecución del proyecto.
- Definir actividades iniciales a realizar para dar inicio al proyecto.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Desarrollo de la reunión:

El Ing. Alexander Díaz responsable del Área de Sistemas y encargado del proyecto dentro de Promociones y Cobranzas Beta S.A., realizó el correspondiente saludo y bienvenida al grupo de trabajo, y da inicio a la reunión.

Acto seguido se procede por parte de los ingenieros Alejandro Torres y Danny López, a informar de las fases contempladas para la realización del proyecto, las cuales se dividen en tres

- Fase 1: Reconocimiento, recolección, y análisis de información estado Inicial, antes de ejecutar plan de concientización.

Actividades a realizar:
- Recolectar la información de la empresa para identificar exposiciones a las que pueda estar expuesto frente a la ingeniería social.
- Realizar encuestas de conocimiento sobre el tema de ingeniería social a los empleados de la empresa.
- Basándose en la información que se reciba por PYCB, definir unas pruebas de ingeniería social y objetivos de dichas pruebas para realizar la ejecución de estas.
- Una vez aprobadas por PYCB las pruebas de ingeniería social planteadas por los ejecutantes, se procederá a ejecutar las mismas.
- realizar un análisis de las encuestas y las pruebas de ingeniería social

- Fase 2: Ejecución de plan de concientización.

Actividades a realizar:
- Basándose en los análisis realizados a las pruebas de ingeniería social y encuestas de la Fase1, realiza un plan de concientización.
- Una vez aprobado el plan de concientización se procede a la ejecución del mismo.

- Fase 3: Reconocimiento, recolección, y análisis de información, estado luego de ejecutar el plan de concientización.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Actividades a realizar

- Realizar una segunda ronda de pruebas de ingeniería social.
- Realizar una segunda encuesta tipo examen.
- Realizar análisis de las pruebas y encuestas realizadas en esta fase y comparar frente al estado inicial.

Luego de la explicación de las fases del proyecto, se habla de la información confidencial de la empresa, que tratamiento se va a dar a esta en la ejecución del proyecto ya que al manejar cobros de una entidad financiera, la información que allí reposa en muchos casos es sensible y confidencial, para lo cual se realizara un acuerdo de confidencialidad, y para el cual el primer Acuerdo de esta acta será diseñado el documento de acuerdo de confidencialidad por los ingenieros Alejandro Torres y Danny López y entregado para el 05 de Agosto de 2016 al ing. Alexander, quien este mismo día lo entregará al área legal de PyCB para que sea revisado avalado y modificado legalmente si corresponde, y el ing Alexander se compromete que para la próxima reunión estará listo dicho acuerdo para que sea firmado por las partes.
adicionalmente la información que sea considerada como confidencial por Promociones y Cobranzas Beta S.A., no podrá ser publicada en el documento de proyecto de grado, a menos de que sea cambiada o puesta en borroso la información crítica de la misma

Se Acuerda en segunda instancia las fases y actividades a realizar dentro de cada una de ellas, como la ejecución del proyecto, y procede a definir como tercer acuerdo entre el ing. Alexander y los ingenieros Alejandro Torres y Danny López, los documentos que serán entregables del proyecto, dentro de los se acuerdan los siguientes:

1. Documento de pruebas a realizar de ingeniería social en Promociones y Cobranzas Beta S.A., y análisis de las pruebas realizadas.
2. Documentos encuestas y análisis de las mismas, para este caso son dos documentos para la fase inicial y dos para la última fase, los documentos de análisis.
3. Documento del Plan de Concientización a desarrollar.
4. Listas de asistencia a capacitaciones.
5. Resultados del plan de concientización.
6. Documento en tipo presentación, manual de concientización sobre la ingeniería social.
7. Video de capacitación basado en la capacitación presencial sobre la ingeniería social. Como este será apoyado por áreas de la empresa será tenido en cuenta como información confidencial, sin embargo, se tomarán pantallazos como evidencia para el proyecto.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Luego de definir los entregables del proyecto para Promociones y Cobranzas Beta S.A. , se valida con el ing. Alexander, la información que nos puede ser entregada para realizar las pruebas de ingeniería social y cuales confidencial, como cuarto acuerdo nos entrega la siguiente información catalogada alguna como confidencial, en el siguiente listado como información entregada por Promociones y Cobranzas Beta S.A.:

- Directorio de Promociones y cobranzas Beta S.A. donde se encuentran nombres de empleados, email, número de teléfono de contacto empresarial extensión si tiene, y en algunos casos número telefónico de celular.
- Organigrama de Promociones y Cobranzas Beta S.A.
- Documentación de la estructura de red, dispositivos, direcciones IP, equipos servidores. Información confidencial.

Finalmente se informa al ing. Alexander, del tema de observación que se realizará en cada reunión, aprovechando que se accede como un proveedor, y a su vez aprovechando el recurso interno el Ing. Alejandro Torres, quien trabaja en el área de sistemas de PyCB

Seguimiento a la Reunión

- Con respecto al acuerdo 1 de la reunión, se acuerda diseñar un documento de acuerdo de confidencialidad entre las partes por parte de los ingeniero Alejandro Torres y Danny López, el cual será entregado el 05 de Agosto de 2016, y será evaluado por el área legal, para ser firmado en la siguiente reunión
- Con respecto al acuerdo 2, se aprueban fases por el ing. Alexander.
- Como acuerdo 3, se definen documentos entregables y confidenciales de la empresa y tratamiento de información confidencial de PyCB.
- Como Acuerdo 4, se reciben los documentos mencionados en esta acta, los cuales solo serán usados por los ejecutores del proyecto para análisis de las pruebas de ingeniería social a realizar y se define cuáles de ellos serán tomados como confidenciales

Acuerdos y compromisos

El día de hoy se reciben los archivos mencionados en este documento de parte del ing. Alexander, Se acuerda revisar nuevamente el avance de los compromisos adquiridos por los miembros de esta reunión una vez se encuentre el documento de pruebas a realizar con el fin de la aprobación del mismo, al igual que firmar el acta de confidencialidad. La próxima reunión será agendada por correo electrónico.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Anexos: - Directorio de Promociones y cobranzas Beta S.A. - Organigrama de Promociones y Cobranzas Beta S.A. - Documentación de la estructura de red, dispositivos, direcciones IP, equipos servidores. La cual será editada en el proyecto con el fin de no revelar direcciones reales de la empresa		
Elaborada por: Alejandro Torres Diaz		Fecha elaboración: 20 de Agosto de 2016 Fecha próxima reunión: Se programara por correo Electrónico

Ing. Alexander – Director de Sistemas	Ing. Alejandro Torres – Ejecutor del proyecto
Ing. Danny López – Ejecutor del proyecto	

Anexo B. Acta de reunión 2

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

ACTA DE REUNIÓN No. 02	
Tema: revisión y aprobación de pruebas de ingeniería social a realizar a Promociones y Cobranzas Beta S.A.	
Nombre de la reunión: APROBACIÓN DE DOCUMENTO DE PRUEBAS DE INGENIERIA SOCIAL EN PROMOCIONES Y COBRANZAS BETA S.A.	
Fecha de la reunión: 09 de Septiembre de 2016	
Lugar de la reunión: Oficina de Sistemas sede principal Bogotá, Promociones y cobranzas Beta S.A.	
Asistentes: Ing. Alexander – Jefe de Sistemas	Ing. Alejandro Torres – ejecutor del proyecto Ing. Danny López – ejecutor del proyecto

Objetivos de la reunión:

- Validar que las pruebas de ingeniería social que se buscan realizar a la empresa, correspondan a lo que está buscando Promociones y Cobranzas Beta S.A. en cuanto a informar y concientizar a sus empleados sobre la amenaza de la ingeniería social.
- Revisar y autorizar, la realización de las pruebas de ingeniería social según se establece en el documento adjunto a esta acta, en donde se definen quienes son las personas que se busca sean objetivos de ataques de las pruebas ingeniería social, y posibles víctimas dentro de un ataque real.
- Firmar acta de confidencialidad entre ambas partes, tanto los ejecutores del proyecto como la empresa Promociones y cobranzas Beta.
- Explicar qué es una Carta de get-out-of-jail y solicitar la misma a Promociones y cobranzas Beta S.A.
- Aprobar dentro de esta acta el inicio y realización de las pruebas de ingeniería social a realizar para Promociones y Cobranzas Beta S.A.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Desarrollo de la reunión:

El Ing. Alexander responsable del Área de Sistemas y encargado del proyecto dentro de Promociones y Cobranzas Beta S.A., realizó el correspondiente saludo y bienvenida al grupo de trabajo, y da inicio a la reunión.

Acto seguido se procede a verificar en el documento de pruebas de ingeniería social a realizar en Promociones y Cobranzas Beta, el cual fue entregado a cada uno de los participantes para su correspondiente lectura, durante esta validación se realiza lo siguiente paso a paso:

1. Se verifica una a una las pruebas de ingeniería social que se buscan realizar. Una vez expuestas cada una de estas pruebas por parte de los ingenieros Alejandro Torres y Danny López, el ing. Alexander Díaz está de acuerdo, y aprueba a que sean estas las pruebas que se realizaran.
2. Se habla sobre el apoyo por parte de sistemas para la realización de dichas pruebas y a su vez que sistemas también será una de las áreas a quienes se realizaran pruebas, dados casos puntuales que se presentan dentro de la empresa como la asignación de permisos no necesarios a ciertos empleados por parte de auxiliares del área.
3. Se exponen las personas que serán objetivos de estas pruebas de ingeniería social iniciales, las cuales también se encuentran descritas en el documento ya entregado con anterioridad, e indicando el motivo por el cual estas personas son objetivos y pueden ser posibles objetivos de este tipo de ataques en casos reales; luego de dicha exposición el ing. Alexander aprueba que dichas pruebas se realicen a estas personas.
4. Se procede a leer el acta de confidencialidad diseñada entre ambas partes, y la cual ya se había entregado mediante correo electrónico en borrador para su posterior lectura, y se aprueba y firma la misma entre ambas partes, acuerdo 1, se firma el documento de confidencialidad entre las partes y de este se sacara una copia de inmediato para que cada uno de los asistentes cuente con una copia firmada, al igual que la empresa para su archivo.
5. Se explica de parte del ing. Danny López el concepto de una carta de get-out-of-jail, que hace referencia a una carta en la que el representante legal de la compañía, presidente o gerente general de la empresa, indica que las personas ejecutoras del proyecto va a proceder con la realización de una pruebas de ingeniería social descritas dentro de la misma carta, y que se encuentran autorizados a realizar las mismas, adicionalmente esta debe contener números de contacto directo con quien autoriza, esta funciona como salvo conducto en caso de que algún empleado en su afán y pro actividad por detener un posible delito contacte a las autoridades competentes y seguridad, para que estas se den por enteradas de la reportarlas a la casa matriz.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Actividad y no pase a inconvenientes mayores para ninguna de las dos partes, al igual que funciona como documento legal para demostrar la realización de dichas pruebas. Una vez explicado el concepto el ing. Alexander indica que procederá a solicitar dicho documento y validará con la el área legal de la empresa para que este sea realizado y aprobado sin problemas, como acuerdo 2. Esta será entregada en físico, una copia para el ing. Alejandro Torres y otra copia para el ing. Danny López, a más tardar en 8 días hábiles.

6. Una vez validada toda la información de la pruebas a realizar, se autoriza dentro de esta acta por parte del ing. Alexander, que las pruebas son las óptimas para validar la problemática dentro de Promociones y Cobranzas Beta S.A. y se autoriza a que estas sean las pruebas que se realizaran, adicionalmente se aprueba dar inicio a las mismas a partir del 01de Agosto de 2016, y una vez ya se cuente a su vez con la carta de get-out-of-jail, adicionalmente el ing. Alexander solicita se le mantenga informado de la realización de dichas pruebas, ya sea telefónicamente o vía correo electrónico.
7. Acuerdo 3. Finalmente se acuerda entre ambas partes, realizar una siguiente reunión de ser necesario para revisar resultados de las pruebas una vez estas sean finalizadas, y el plan de concientización diseñado luego de estas.

Seguimiento a la Reunión

- Con respecto al acuerdo 1 de la reunión, se firma el documento de confidencialidad entre las partes y de este se sacara una copia de inmediato para que cada uno de los asistentes cuente con una copia firmada, al igual que la empresa para su archivo.
- Con respecto al acuerdo 2, el ing. Alexander se compromete a entregar en no más de 8 días hábiles la carta de get-out-of-jail a los ingenieros Alejandro Torres y Danny López, una copia para cada uno.
- Como acuerdo 3, implícito en las demás actividades de esta reunión, se aprueba por parte de Promociones y cobranzas Beta S.A. la realización de la pruebas de ingeniería social propuestas por los ingenieros ejecutantes Alejandro Torres y Danny López, las cuales podrán ser iniciadas a partir del 01 de Agosto de 2016 y una vez se cuente con la carta de salvo get-out-of-jail, adicionalmente se acuerda que antes de ejecutar la acción de una prueba de ingeniería social se informara telefónicamente o vía mail de la realización de la misma al ingeniero Alexander.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Acuerdos y compromisos Se acuerda revisar nuevamente el avance de los compromisos adquiridos por los miembros de esta reunión una vez sean culminadas las pruebas de ingeniería social y se encuentre listo un borrador del plan de concientización para validación del mismo. También se mantendrá informado al Ing. Alexander de la realización de la pruebas antes de su ejecución. De igual manera él envió del acta a todos los miembros para su conocimiento y aprobación.
Anexos: Documento de pruebas de ingeniería social a realizar en Promociones y Cobranzas Beta.

Elaborada por: Danny Juan Pablo López Rodriguez		Fecha elaboración: 19 de Agosto de 2016
		Fecha próxima reunión: Se programara por correo

Ing. Alexander – Jefe de Sistemas	Ing. Alejandro Torres – Ejecutor del proyecto
Ing. Danny López – Ejecutor del proyecto	

Anexo C. Acta de reunión 3

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

ACTA DE REUNION No. 03	
Tema: revisión y aprobación de plan de concientización para Promociones y Cobranzas Beta S.A.	
Nombre de la reunión: APROBACIÓN DEL PLAN DE CONCIENTIZACIÓN EN PROMOCIONES Y COBRANZAS BETA S.A.	
Fecha de la reunión: 20 de septiembre de 2016	
Lugar de la reunión: Oficina de Sistemas sede principal Bogotá, Promociones y cobranzas Beta S.A.	
Asistentes: Ing. Alexander – Jefe de Sistemas	Ing. Alejandro Torres – ejecutor del proyecto Ing. Danny López – ejecutor del proyecto

Objetivos de la reunión:

- Validar el plan de concientización para Promociones y Cobranzas Beta S.A. en cuanto a informar y concientizar a sus empleados sobre la amenaza de la ingeniería social.
- Revisar y autorizar, la ejecución del plan de concientización según se establece en el documento adjunto a esta acta.
- Firmar esta acta como documento de aprobación y autorización para el plan de concientización, tanto los ejecutores del proyecto como la empresa Promociones y cobranzas Beta.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Desarrollo de la reunión:

El Ing. Alexander responsable del Área de Sistemas y encargado del proyecto dentro de Promociones y Cobranzas Beta S.A., realizó el correspondiente saludo y bienvenida al grupo de trabajo, y da inicio a la reunión.

Acto seguido se procede a verificar en el documento del plan de concientización a ejecutar en Promociones y Cobranzas Beta, el cual fue entregado a cada uno de los participantes para su correspondiente lectura, durante esta validación se realiza lo siguiente paso a paso:

1. Se verifica una a una las actividades y acciones del plan de concientización. Una vez expuestas cada una de las actividades por parte de los ingenieros Alejandro Torres y Danny López, el ing. Alexander Díaz está de acuerdo, y aprueba a que sean estas las actividades a realizar.
2. Se habla sobre el apoyo por parte de sistemas para la realización de dichas actividades.

Seguimiento a la Reunión

- Con respecto al acuerdo 1 de la reunión, se firma este documento como aprobación y entrega de cada una de las actividades del plan de concientización expuesto.

ACTA DE REUNIÓ PARA EL PROYECTO DE GRADO LLAMADO: DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.

Acuerdos y compromisos Se mantendrá informado al Ing. Alexander de la realización de las pruebas antes de su ejecución. De igual manera él envió del acta a todos los miembros para su conocimiento y aprobación.		
Anexos: Documento de plan de concientización		
Elaborada por: Danny Juan Pablo López Rodriguez		Fecha elaboración: 20 de septiembre de 2016
		Fecha próxima reunión: Se programará por correo de ser necesaria

Ing. Alexander – Jefe de Sistemas	Ing. Alejandro Torres – Ejecutor del proyecto
Ing. Danny López – Ejecutor del proyecto	

Anexo D. Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD

Entre los suscritos a saber, en primera parte OSWALDO ALEJANDRO TORRES DIAZ, Mayor de edad y domiciliado en Funza, identificado(a) como aparece al lado de su respectiva firma y al final de este documento, quien actúa en nombre propio; en segunda parte DANNY JUAN PABLO LÓPEZ RODRIGUEZ, Mayor de edad y domiciliado en Bogotá D.C., identificado(a) como aparece al lado de su respectiva firma y al final de este documento, quien actúa en nombre propio, y finalmente por otra parte, HÉCTOR MARIO AMAR GARZÓN, también mayor de edad, domiciliado en Bogotá D.C, identificado(a) como aparece al pie de su firma y al final de este documento, quien actúa a nombre de PROMOCIONES Y COBRANZAS BETA S.A., se ha acordado celebrar el presente acuerdo de confidencialidad que se regirá por las siguientes cláusulas:

CONSIDERACIONES

1. Las partes están interesadas en preservar, mantener y salvaguardar de forma segura la información recolectada de cada uno de las pruebas de ingeniería social a nivel de seguridad informática realizadas a PROMOCIONES Y COBRANZAS BETA S.A.
2. Debido a la naturaleza del proyecto, se hace necesario que estas partes puedan llegar a manejar información confidencial de PROMOCIONES Y COBRANZAS BETA S.A., relacionada con usuarios de los servicios brindados en su naturaleza de negocio o información de sus trabajadores, información sujeta a derechos de propiedad intelectual durante y en la etapa posterior a la elaboración del proyecto DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A. suscrito por OSWALDO ALEJANDRO TORRES DIAZ y DANNY JUAN PABLO LÓPEZ RODRIGUEZ.

CLÁUSULAS

PRIMERA. OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información recolectada, o intercambiada entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información de clientes o trabajadores, estadísticas, o cualquier información revelada sobre terceras personas.

SEGUNDA. CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, publicada, facilitada o creada entre ellas en el transcurso del tiempo de la elaboración del proyecto y 15 años más a partir de la finalización del proyecto, será mantenida en escrita confidencialidad. La parte receptora correspondiente solo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata o las autoridades competentes mediante una orden judicial emitida por un juez de garantías.

Anexo E. Get out of jail

A QUIEN CORRESPONDA

Promociones y Cobranzas Beta S.A.

Bogotá, agosto 01 de 2016

Conociendo la actividad a la que se dedica Promociones y Cobranzas Beta S.A., la siguiente carta expresa que los ingenieros OSWADLO ALEJANDRO TORRES DIAZ identificado con cedula de ciudadanía número 79730882 y DANNY JUAN PABLO LÓPEZ RODRIGUEZ identificado con cedula de ciudadanía número 80791860, se encuentran autorizados para realizar las siguientes pruebas de seguridad informática enfocadas a la Ingeniería Social:

- Phishing.
- Baiting.
- Pretexting.
- Dumpster diving.
- Shoulder Surfing.
- Validación de información en redes sociales.

Dichas pruebas solo serán ejecutadas a nivel interno de la empresa Promociones y Cobranzas Beta S.A. y a sus empleados, sin que en algún momento se llegue a usar la información obtenida para fines diferentes a muestra de evidencia de falencias de seguridad encontradas.

En caso de que alguna autoridad de seguridad, legal o Autoridades competentes sea reportada, esta carta libera de responsabilidad a los ingenieros mencionados en esta, ya que se encuentran autorizados por la empresa para realizar las pruebas en mención.

Atentamente,

_____

Jefe de Sistemas de Promociones y Cobranzas Beta S.A.

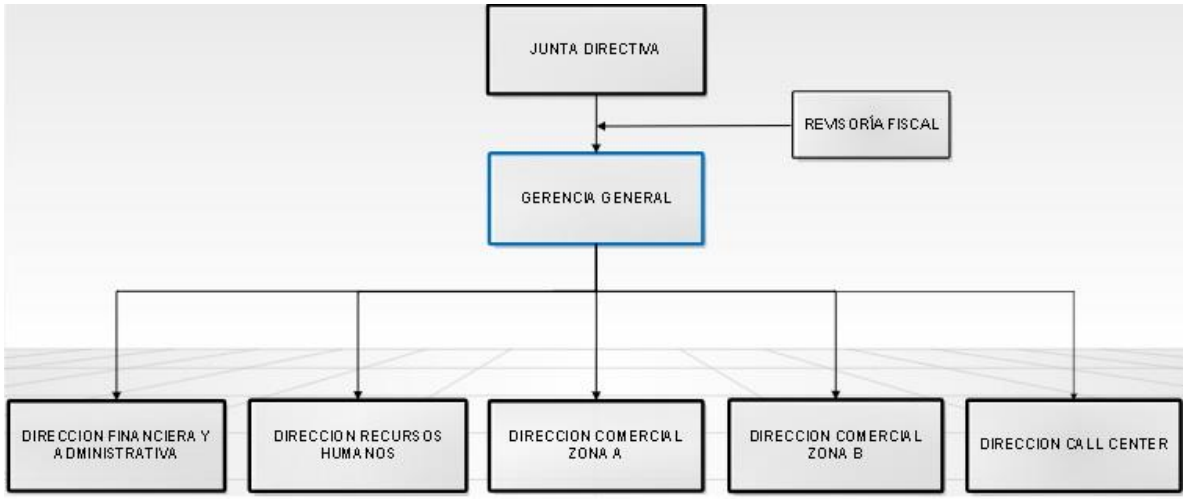
Celular: 3174368153

Teléfono: 3144777 - 7427615- 3572290 Ext: 601

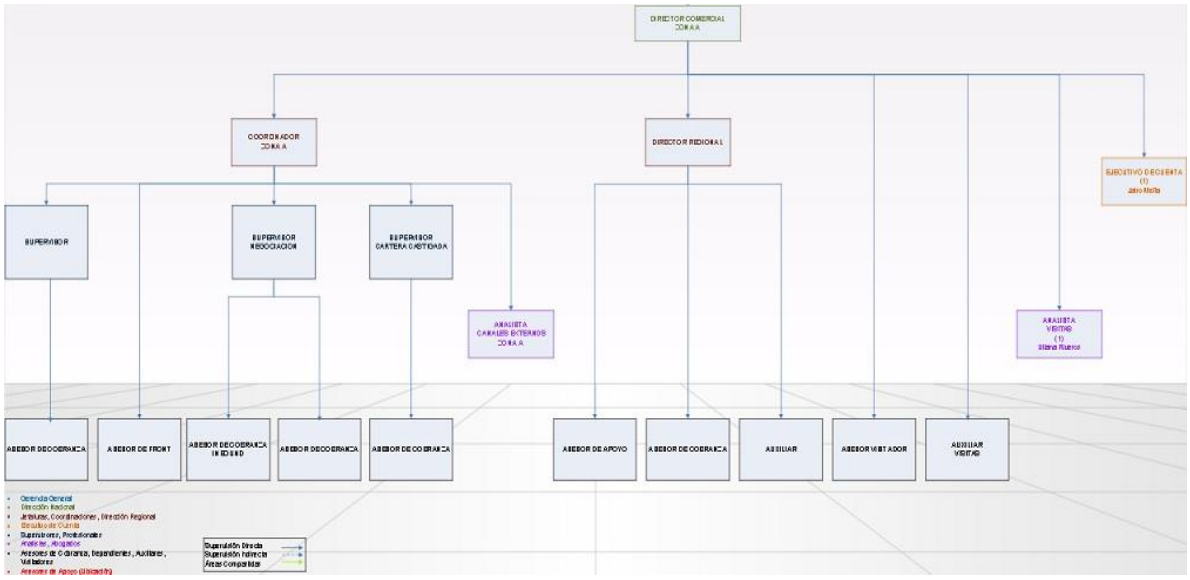
Email: adiaz@cobranzasbeta.com.co

Anexo F. Documentos entregados por Promociones Y Cobranzas Beta

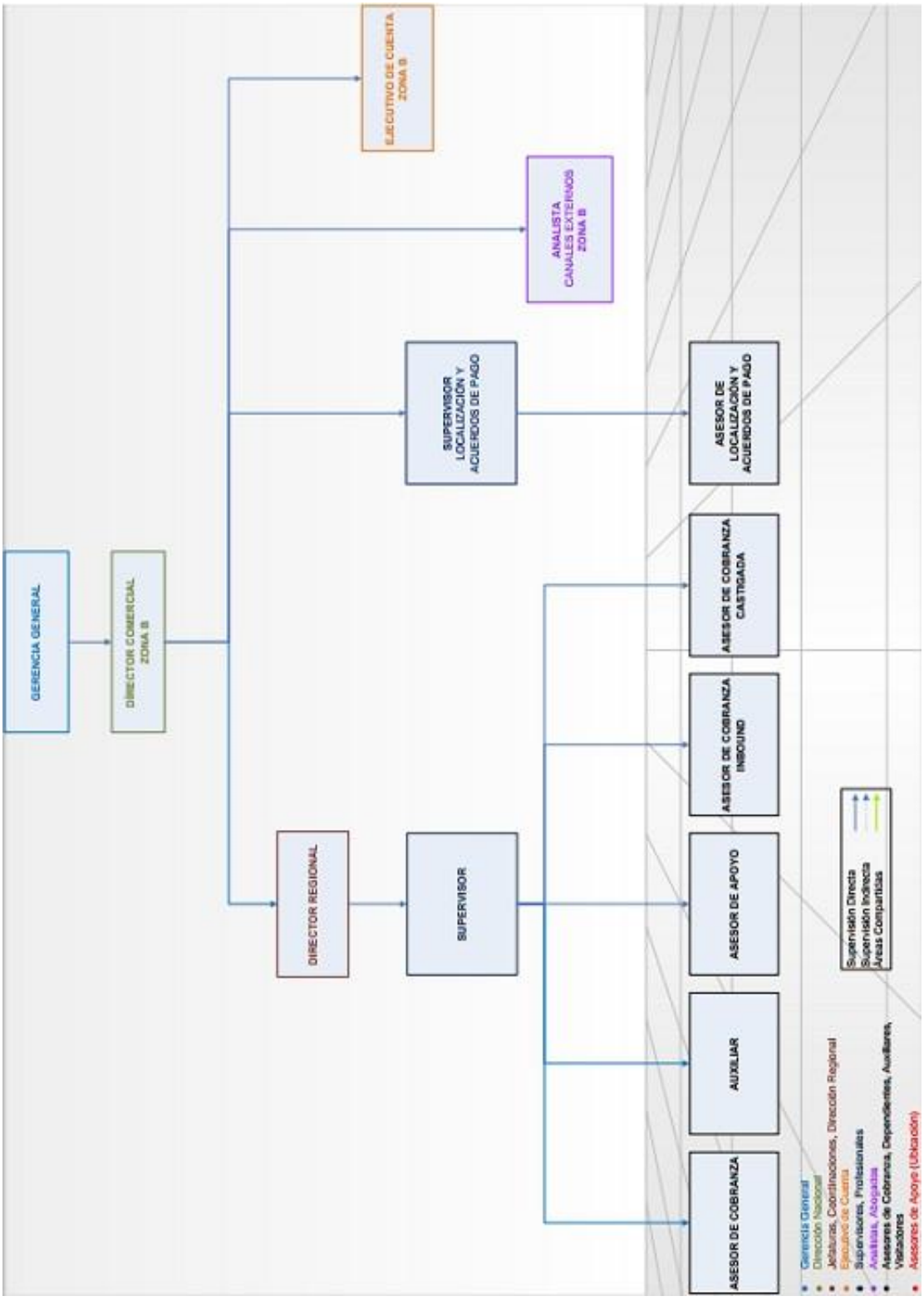
F.1 Organigrama Primer Nivel



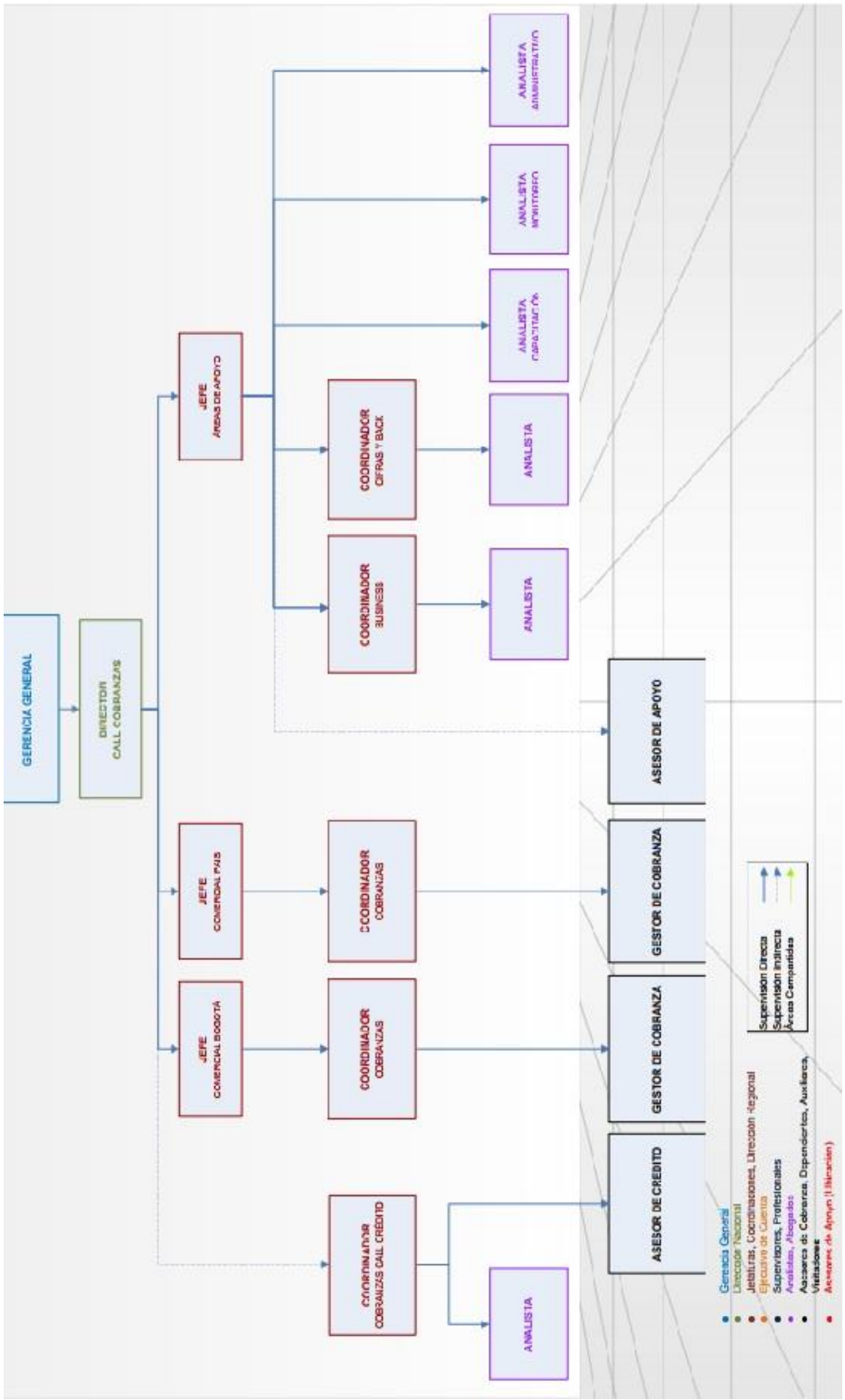
F.2 Organigrama Zona A



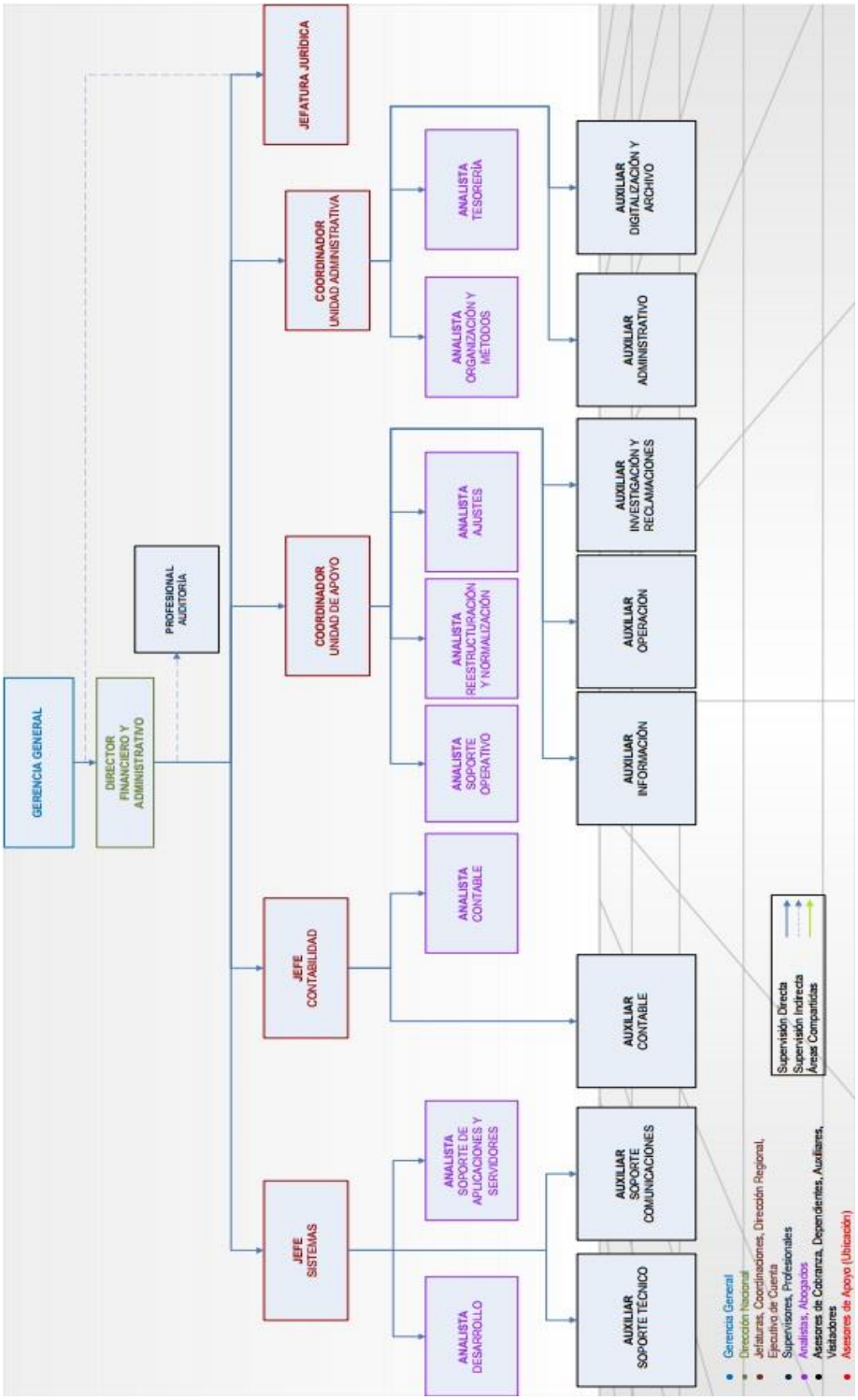
F.3 Organigrama Zona B



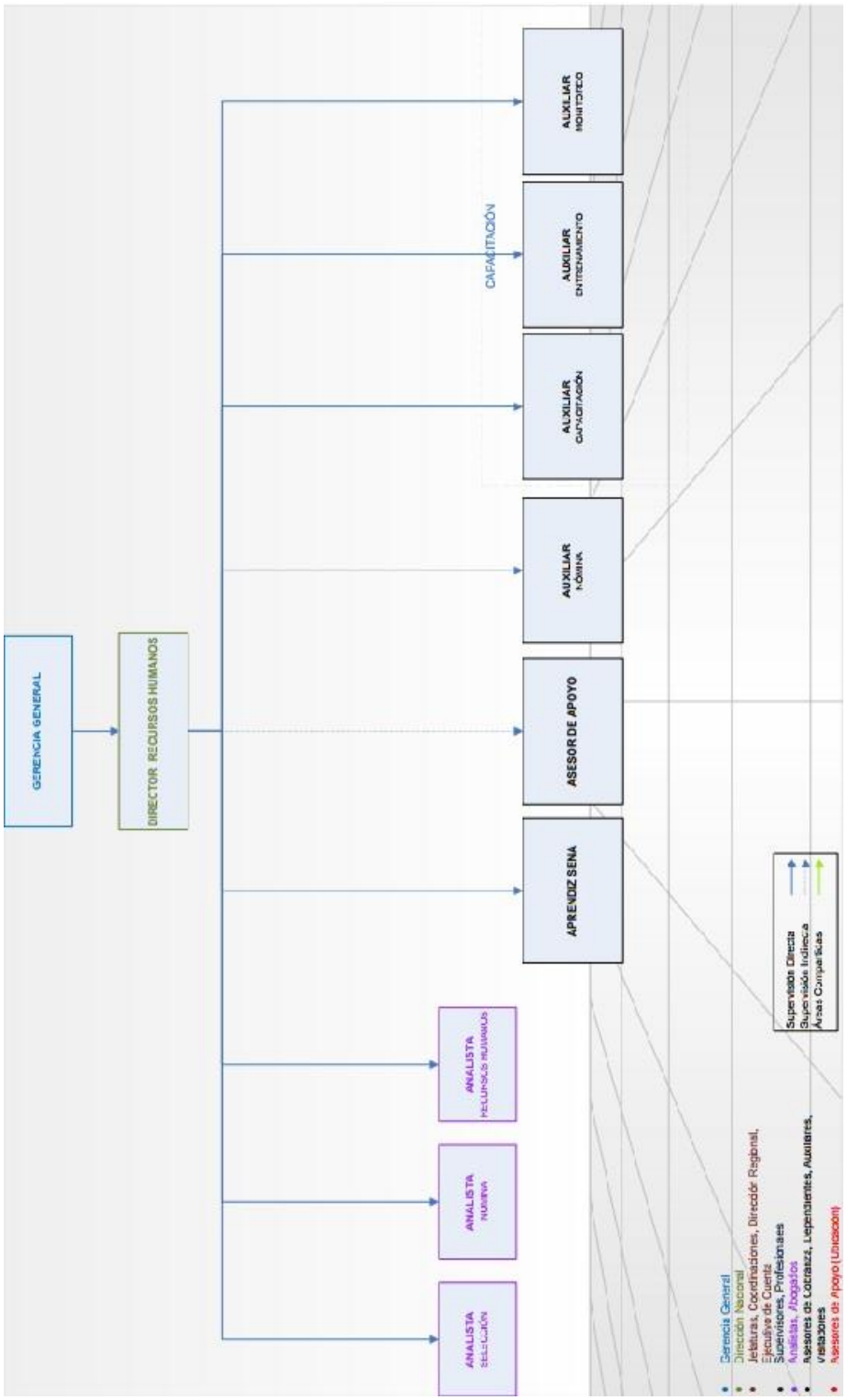
F.4 Organigrama call center



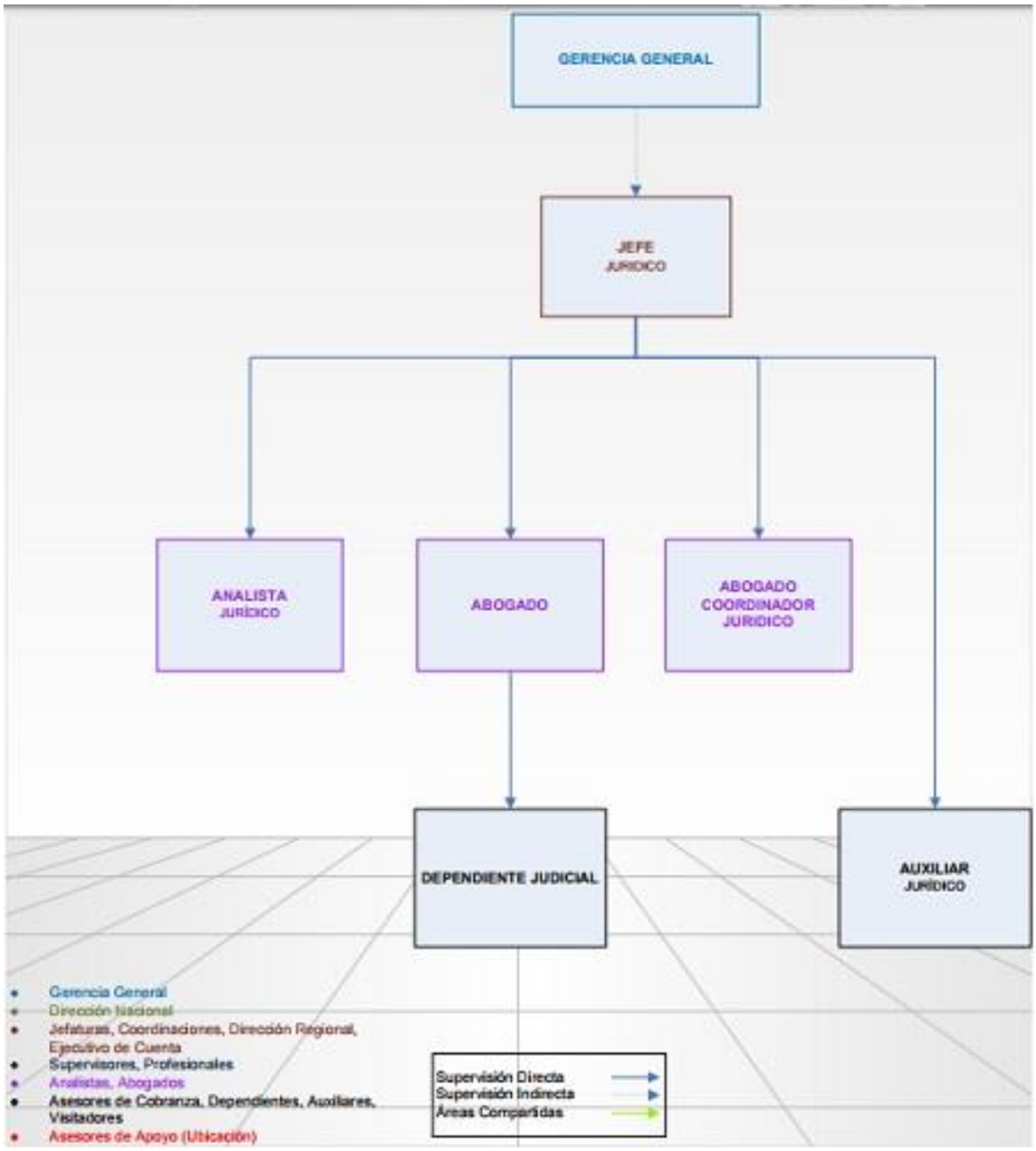
F.5 Organigrama dirección administrativa



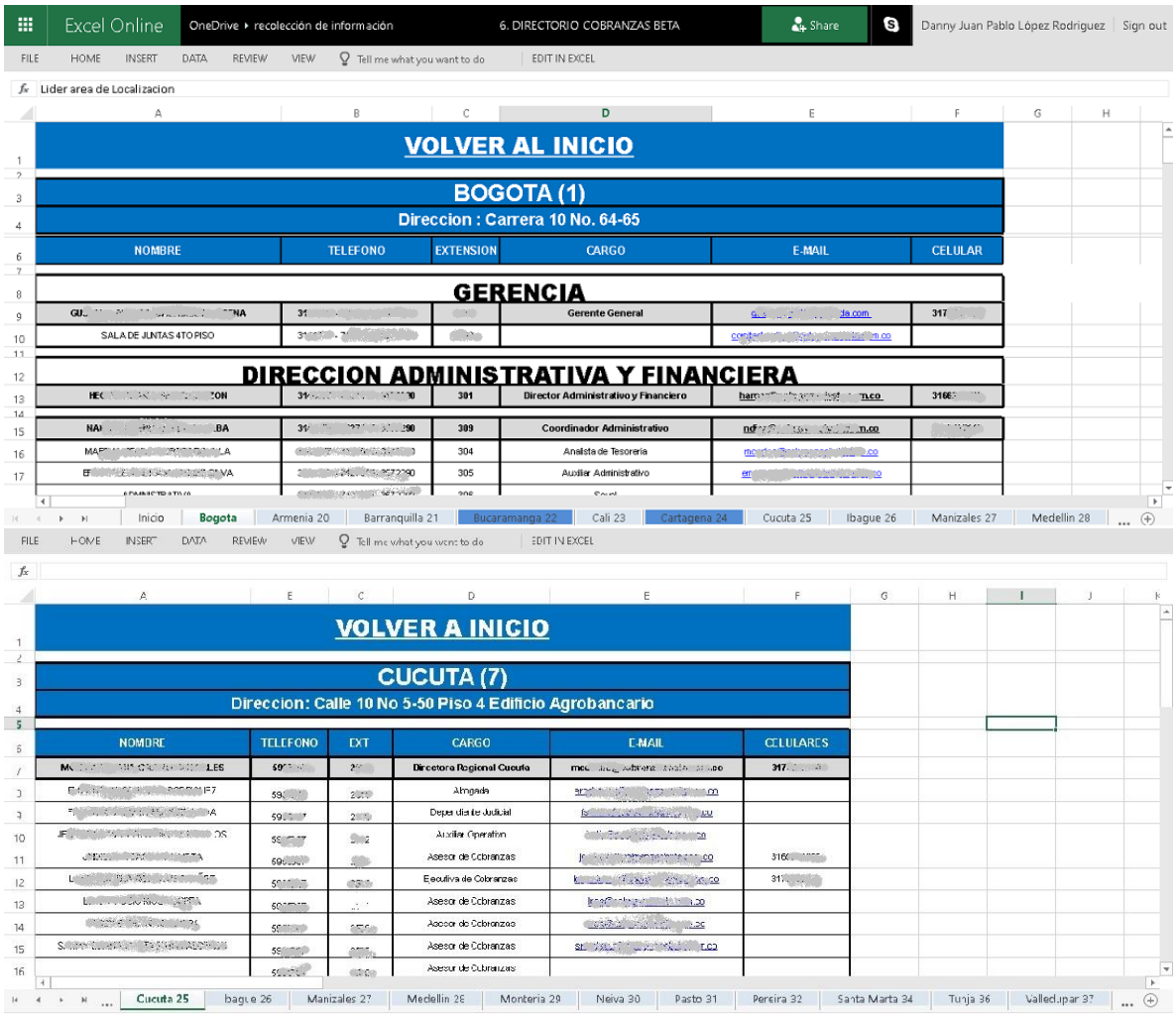
F.6 Organigrama dirección de recursos humanos



F.7 Organigrama jurídico



F.8 Directorio Promociones y Cobranzas Beta



VOLVER AL INICIO

BOGOTA (1)

Direccion : Carrera 10 No. 64-65

NOMBRE	TELEFONO	EXTENSION	CARGO	E-MAIL	CELULAR
GERENCIA					
[illegible]	31[illegible]	[illegible]	Gerente General	[illegible]	317[illegible]
SALA DE JUNTAS 4TO PISO	31[illegible]	[illegible]		[illegible]	
DIRECCION ADMINISTRATIVA Y FINANCIERA					
[illegible]	31[illegible]	301	Director Administrativo y Financiero	[illegible]	3166[illegible]
[illegible]	31[illegible]	309	Coordinador Administrativo	[illegible]	[illegible]
[illegible]	[illegible]	304	Analista de Tesoreria	[illegible]	
[illegible]	[illegible]	305	Auxiliar Administrativo	[illegible]	

Inicio | Bogota | Armenia 20 | Barranquilla 21 | Bucaramanga 22 | Cali 23 | Cartagena 24 | Cucuta 25 | Ibague 26 | Manizales 27 | Medellin 28

VOLVER A INICIO

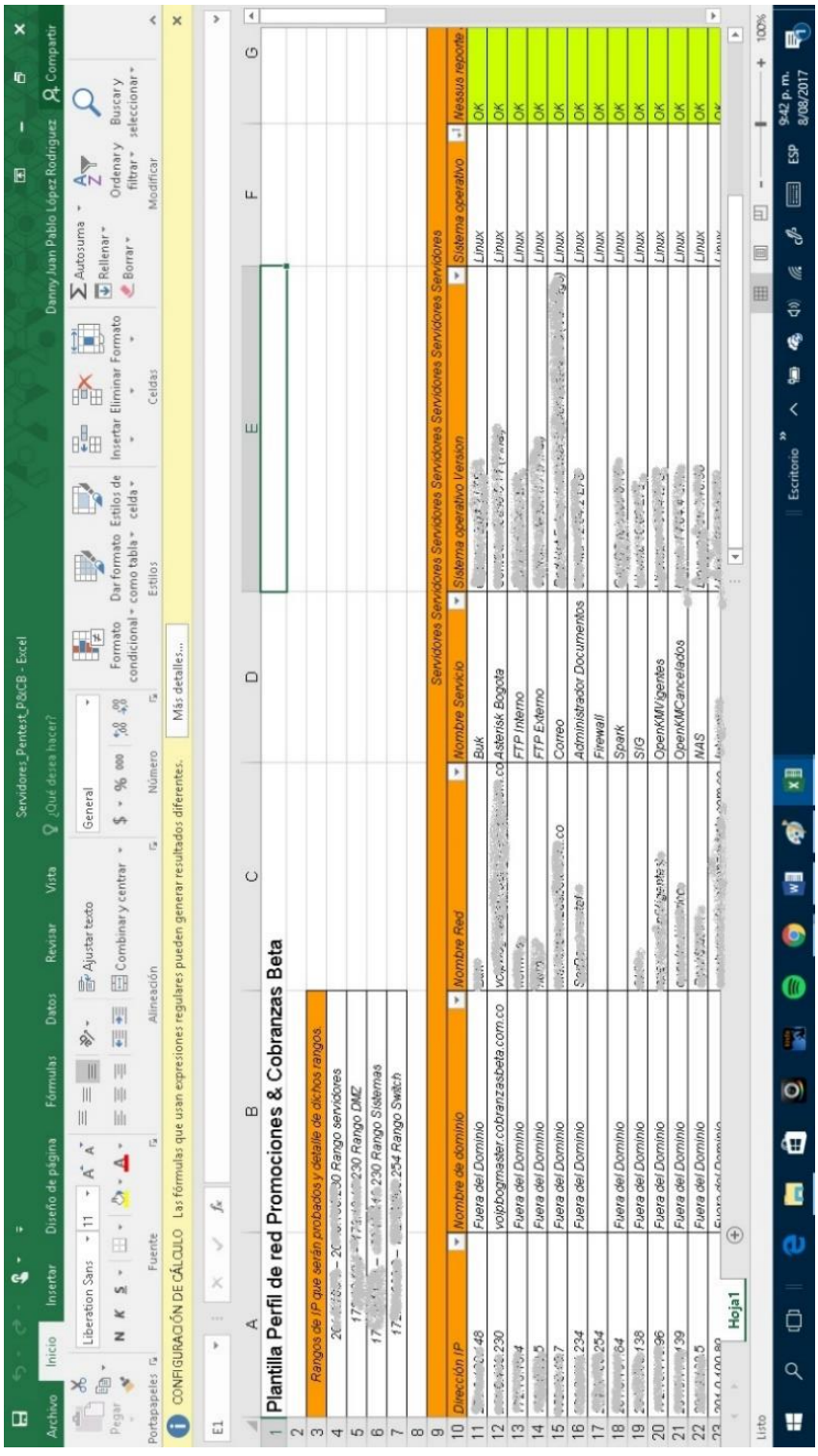
CUCUTA (7)

Direccion: Calle 10 No 5-50 Piso 4 Edificio Agrobancario

NOMBRE	TELEFONO	EXT	CARGO	E-MAIL	CELULARES
[illegible]	59[illegible]	[illegible]	Directora Regional Cucuta	[illegible]	317[illegible]
[illegible]	59[illegible]	[illegible]	Almacén	[illegible]	
[illegible]	59[illegible]	[illegible]	Depe cliente Judicial	[illegible]	
[illegible]	59[illegible]	[illegible]	Auxiliar Operativo	[illegible]	
[illegible]	59[illegible]	[illegible]	Asesor de Cobranzas	[illegible]	3166[illegible]
[illegible]	59[illegible]	[illegible]	Ejecutiva de Cobranzas	[illegible]	317[illegible]
[illegible]	59[illegible]	[illegible]	Asesor de Cobranzas	[illegible]	
[illegible]	59[illegible]	[illegible]	Asesor de Cobranzas	[illegible]	
[illegible]	59[illegible]	[illegible]	Asesor de Cobranzas	[illegible]	
[illegible]	59[illegible]	[illegible]	Asesor de Cobranzas	[illegible]	

Cucuta 25 | Ibague 26 | Manizales 27 | Medellin 28 | Monteria 29 | Neiva 30 | Pasto 31 | Pereira 32 | Santa Marta 34 | Tunja 36 | Valledupar 37

F.9 Documentación de la red



Plantilla Perfil de red Promociones & Cobranzas Beta

Rangos de IP que serán probados y detalle de dichos rangos.					
[redacted] – [redacted]30 Rango servidores					
[redacted] – [redacted]230 Rango DMZ					
[redacted] – [redacted]230 Rango Sistemas					
[redacted] – [redacted]254 Rango Switch					

Servidores Servidores Servidores Servidores Servidores Servidores Servidores Servidores					
Dirección IP	Nombre de dominio	Nombre Red	Nombre Servicio	Sistema operativo Version	Sistema operativo	Nessus reporte
[redacted]48	Fuera del Dominio	[redacted]	Buk	[redacted]	Linux	OK
[redacted]230	volpbogmaster.cobranzasbeta.com.co	[redacted].co	Asterisk Bogota	[redacted]	Linux	OK
[redacted]4	Fuera del Dominio	[redacted]	FTP Interno	[redacted]	Linux	OK
[redacted]5	Fuera del Dominio	[redacted]	FTP Externo	[redacted]	Linux	OK
[redacted]7	Fuera del Dominio	[redacted].co	Correo	[redacted]	Linux	OK
[redacted]234	Fuera del Dominio	[redacted]	Administrador Documentos	[redacted]	Linux	OK
[redacted]254			Firewall		Linux	OK
[redacted]64	Fuera del Dominio		Spark	[redacted]	Linux	OK
[redacted]138	Fuera del Dominio	[redacted]	SIG	[redacted]	Linux	OK
[redacted]96	Fuera del Dominio	[redacted]	OpenKMVigentes	[redacted]	Linux	OK
[redacted]139	Fuera del Dominio	[redacted]	OpenKMCancelados	[redacted]	Linux	OK
[redacted]5	Fuera del Dominio	[redacted]	MAS	[redacted]	Linux	OK
[redacted]	Fuera del Dominio	[redacted]	[redacted]	[redacted]	Linux	OK

Anexo G. Listas de asistencia

G.1 Lista de asistencia 1

Promociones y Cobranzas Beta S.A.

Grupo 01

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

FECHA: 11 de Noviembre de 2016

Nº	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1030904305	DUQUE GARAVITO LUIS FELIPE	ASESOR DE COBRANZAS T.F	Indefinido	Felipe Duque.
2	1030654482	ABRIL MONTAÑEZ MARIANO	ASESOR DE COBRANZAS		
3	86452132	COTES RODRIGUEZ DAVID ENRIQUE	ANALISTA OPERATIVO		
4	52443534	RIVEROS ROMERO JENNY LILIANA	ANALISTA CIFRAS T.F	Fijo	
5	1026598508	RODRIGUEZ VARGAS CESAR SANTIAGO	ASESOR DE COBRANZAS T.F	Fijo	
6	1233890043	RODRIGUEZ GAITAN JOSE LUIS	ASESOR DE COBRANZAS T.F	Fijo	
7	1018500899	PRADA MELO ANGIE TATIANA	ASESOR DE COBRANZAS T.F	Fijo	
8	80212791	GALEANO MOLINA ORLANDO ALEXAND	ASESOR DE COBRANZAS	Indefinido	
9	53061965	PEDREROS DIAZ MARTA LILIANA	SUPERVISOR		
10	80112364	MORALES SUAREZ ALEXANDER PHYNT	ASESOR DE COBRANZAS		
11	1032383479	MARTINEZ ALARCON FLORA YASMITH	ASESOR DE COBRANZAS T.F	Fijo	
12	1022932301	GARAVITO ALARCON LEIDY CATALINA	ASESOR DE COBRANZAS T.F	Fijo	
13	1030627115	CUERVO CHAUX TANIA SHIRLEY	ASESOR DE COBRANZAS		
14	1020779659	UMAÑA ZABALA CAMILO ANDRES	ASESOR DE COBRANZAS T.F		
15	1007773543	PAEZ GUERRERO KATHERIN ANDREA	ASESOR DE COBRANZAS T.F	Fijo	
16	1032427289	GOMEZ RODRIGUEZ ANGYE LIZETH	ASESOR DE COBRANZAS	Indefinido	
17	1030335690	RAMIREZ ROJAS ANGELICA LILIAN	ASESOR DE COBRANZAS	Indefinido	
18	1074928584	PEDRAZA VEGA ROBINSON IVAN	ASESOR DE COBRANZAS	Indefinido	
19	25280372	MUÑOZ MUÑOZ CONCEPCION	ASESOR DE COBRANZAS		
20	28689110	RAMOS CARDENAS ANGELA MARCELA	COORDINADOR UNIDAD DE APOYO		
21	1033706544	SANCHEZ ORTIZ LORENA	ASESOR DE COBRANZAS T.F	Fijo	
22	1073160546	ORTEGA RODRIGUEZ CAMILO ANDRES	ASESOR DE COBRANZAS T.F		
23	1019058947	TORRES RAMOS LUIS DANIEL	ASESOR DE COBRANZAS T.F	Fijo	
24	1024491895	VELANDIA CORREA DAYIBE ELIZABET	ASESOR DE COBRANZAS		
25	80778659	BUENO JUAN CARLOS	ASESOR DE COBRANZAS		
26	1019073165	CALDERON PACHECO FABIAN HUMBERTO	ASESOR DE COBRANZAS		
27	88144994	MEJIA PORTILLO JAIRO LEONARDO	EJECUTIVO DE CUENTA - COMERCIA		
28	1072656055	QUEVEDO BARBOSA WILLIAM ALBERTO	ASESOR DE COBRANZAS	Indefinido	
29					
30					
31					
32					
33					

Página 1

Grupo 02

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

FECHA: 11 de Noviembre de 2016

Nº	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	31468616	CEBALLOS RODRIGUEZ DEISY	ASESOR DE COBRANZAS	Indefinido	Deicy Ceballos R
2	79291798	SANTAFE RODRIGUEZ OSCAR	ANALISTA DE AJUSTES		
3	1016045865	MORENO FORERO JHON DAVID	ASESOR DE COBRANZAS T.F		
4	1022403548	FLORIDO QUINTANA INGRID DAYANA	ASESOR DE COBRANZAS T.F		
5	1020815115	VARGAS SILVA EDNA LICED	ASESOR DE COBRANZAS T.F		
6	1032388947	CASTRO RICO CLAUDIA MELISA	SUPERVISOR		
7	1014177570	BENITEZ YEPES OMAR HARVEY	ASESOR DE COBRANZAS	Indefinido	
8	1032471596	BARBOSA HERNANDEZ CRISTIAN CAMILO	ASESOR DE COBRANZAS	Indefinido	
9	1010215138	ALCALA ALCALA MAYRA ALEJANDRA	ASESOR DE COBRANZAS	Indefinido	Mayra Alcala
10	1019071352	SANCHEZ BUSTOS EDWIN FERLEY	AUXILIAR OPERATIVO		
11	1015405778	MONTENEGRO PARRA NURY PILAR	ASESOR DE COBRANZAS T.F	Fijo	Nury Montenegro
12	52836430	GUERRERO BULLA DERLY YASBETH	ASESOR DE COBRANZAS	Indefinido	Derly Guerrero
13	52169091	MORALES RENGIFO MARITZA ELENA	COORDINADOR COBRANZAS		
14	1015424879	LARA MORALES WENDY TATIANA	ASESOR DE COBRANZAS	Indefinido	Tatiana Lara M
15	39534210	MORALES REBOLLEDO ROSA	ASESOR APOYO (C.P)		
16	52883265	ROZO GARCES SUANY YUBERLY	ASESOR APOYO (C.P)		
17	53005600	JIMENEZ MORENO ANA YOMARA	ASESOR DE COBRANZAS	INDEFINIDO	
18	52344683	GUZMAN RENDON MAGDA ROCIO	ASESOR DE COBRANZAS	INDEFINIDO	
19	52147064	PEREIRA HERRERA JANETH BEATRIZ	AUXILIAR OPERATIVO	Indefinido	
20	1032418231	RODRIGUEZ CEPEDA SEBASTIAN	ASESOR DE COBRANZAS T.F		
21	1018436394	RIVERA GARCIA JULIE MARCELA	ASESOR DE COBRANZAS T.F		
22	1022369584	CASTRO ARIZA BRIGITTE TATIAN	ASESOR DE COBRANZAS T.F	Fijo	Tatiana Castro A.
23	1032457644	MACCHI AMORTEGUI ERIK GIOVANNY	ASESOR DE COBRANZAS T.F	Fijo	
24	1022394369	VILLAMIZAR CARDENAS JEAN PAUL	ASESOR DE COBRANZAS T.F	Fijo	
25	1010172424	QUINTERO GARCIA KAREN VIVIANA	ASESOR APOYO (C.P)		
26	1030626992	MANRIQUE ARIAS ANA MILENA	ASESOR DE COBRANZAS		
27	52479949	RODRIGUEZ BEJARANO AIDA MARITZA	ASESOR DE COBRANZAS	Indefinido	Maritza Rodriguez
28	52333136	CUBILLOS JIMENEZ DORIS ROCIO	AUXILIAR OPERATIVO	Indefinido	
29	37322932	Yanta Cecilia Serrano S.	Asesor de Cobranzas	Indefinido	
30	1073695585	Jaxiany Sanchez Cobos	Asesor de cobranzas	Indefinido	
31	39789221	YOLANDA BOLIVAR PRADENAS	ASESOR COBRANZAS	INDEFINIDO	
32	1015494697	Jelson Ferney Urresti Valdes	Asesor de cobranzas	Fijo	Jelson Ferney
33	1233499304	Diego Alejandro Mateus Gonzalez	Aprendiz sena	Aprendizaje	Diego Mateus G.
34	99010608453	Alvaro Javier Gonzalez Rodriguez	Aprendiz Sena	Aprendizaje	Javier Gonzalez
35	99071908074	Karina Paola Ospina Diaz	Aprendiz sena	Aprendizaje	

Página 1

Grupo 03

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

FECHA: 11 de Noviembre de 2016

N°	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	52805203	ROBAYO MERCHAN LUZ MARY	ASESOR DE COBRANZAS		
2	52853420	CASTANEDA MATAMOROS IVONNE MARITZA	ANALISTA ZONA B		
3	80176959	SANDOVAL NARANJO JUAN PABLO	SUPERVISOR		
4	51677061	FLOREZ IBARBUEN LUZ DARY	ASESOR DE COBRANZAS	Indefinido	
5	39574824	PULIDO MANRIQUE DIANA MILENA	AUXILIAR OPERATIVO	Indefinido	Diana Pulido
6	1073691585	SANCHEZ COBOS JOXIANY	ASESOR DE COBRANZAS		
7	53053283	VARGAS BRIJALDO JULIANA	EJECUTIVO DE CUENTA - COMERCIA	Indefinido	
8	1030529645	QUIROGA MENDOZA SANDRA MILENA	ASESOR DE COBRANZAS		
9	39782275	BOLIVAR CARDENAS YOLANDA	ASESOR DE COBRANZAS		
10	51652781	LOPEZ VELOZA ALEIDA	ASESOR APOYO (C.P)		
11	1019029236	DIAZ LOPEZ JENNI PAOLA	ASESOR DE COBRANZAS T.F	Fijo.	Paola Lopez
12	1072650143	ARTEAGA URREGO CATHERIN DAYANA	ASESOR DE COBRANZAS T.F	Fijo	Catherin Arteaga
13	1030582994	RUGELES BARRETO MARIA ALEJANDRA	ASESOR DE COBRANZAS T.F	INDEFINIDO	
14	1024468256	VARGAS CUBILLOS LUIS HERNANDO	ASESOR DE COBRANZAS		
15	36069286	SANCHEZ ESTRELLA CLAUDIA MILENA	ASESOR DE COBRANZAS	INDEFINIDO	CLAUDIA
16	1016030959	JIMENEZ VELASQUEZ INGRID YISSED	ASESOR DE COBRANZAS	INDEFINIDO	INGRID JIMENEZ
17	52265586	GOMEZ BECERRA LUZ ANGELA	DIRECTOR COMERCIAL ZONA B		
18	52445752	BONILLA ORTIZ LIBIA XIOMARA	ANALISTA ZONA A		
19	37322952	SANGUINO TRILLOS MARTA CECILIA	ASESOR DE COBRANZAS	Indefinido	
20	1014238135	BAEZ GONZALEZ JUAN SEBASTIAN	ASESOR DE COBRANZAS		
21	52791054	CHAVEZ CUBILLOS VIVIANA	ASESOR DE COBRANZAS	INDEFINIDO	
22	52396386	RODRIGUEZ VELASQUEZ ANGELICA	AUXILIAR OPERATIVO	INDEFINIDO	
23	1030542709	MORA ESPINOSA INGRY KATHERINE	ASESOR DE COBRANZAS T.F	Fijo	
24	1022399534	MORENO CONTRERAS MARIA FERNANDA	ASESOR DE COBRANZAS T.F	FIJO	
25	1019066041	DIAZ ZEA KATY MARICEL	ASESOR DE COBRANZAS T.F	Fijo	
26	65496928	MORALES REBOLLEDO ALBA CECILIA	SUPERVISOR	Indefinido	
27	51856057	MARTINEZ ARCHILA PATRICIA	ASESOR DE COBRANZAS		
28	52155714	MORA RINCON INGRID BRIGITTE	AUXILIAR OPERATIVO	Indefinido	
	53471069	Pereira Herrera Sandra	Aux Operativo	Indefinido	

Grupo 04

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

FECHA: 11 de Noviembre de 2016

Nº	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1136879507	VASQUEZ ROA CATALINA ANDREA	ASESOR DE COBRANZAS T.F		
2	1019017368	BERMUDEZ HERNANDEZ MARLEN VIVIANA	ASESOR DE COBRANZAS T.F	FIJO	
3	1064991324	MUÑOZ JIMENEZ SANDRA PAOLA	ASESOR DE COBRANZAS T.F	Fijo	
4	1023865285	VELANDIA MORA EDWIN CAMILO	ASESOR DE COBRANZAS T.F		
5	1026289296	MENDEZ DELGADO ANGIE LORENA	ASESOR DE COBRANZAS T.F	Fijo	Lorena Mendez
6	1019049477	COBOS GARCIA DIANA CAROLINA	ASESOR DE COBRANZAS		
7	30325819	GONZALEZ DIAZ LINA MARIA	DIRECTOR COMERCIAL ZONA A		
8	52309043	GUERRERO ROJAS NANCY STELLA	SUPERVISOR		
9	1016011370	LEAL RINCON NATHALY	ASESOR DE COBRANZAS		
10	9536821	MORENO RONDON OSCAR JAVIER	ASESOR DE COBRANZAS		
11	53072575	RAMIREZ CAICEDO DIANA MARCELA	ASESOR DE COBRANZAS		
12	1073629123	MONCADA CORTES GINA ROCIO	ASESOR DE COBRANZAS	Indefinido	Gina Moncada C.
13	79709430	RODRIGUEZ MORENO OSCAR ARTURO	AUXILIAR OPERATIVO		
14	1126596816	BERNAL GOMEZ NANCY BRIGITH	ASESOR DE COBRANZAS T.F	Fijo	
15	1016038448	SANABRIA RUBIANO MARIA XIMENA	ASESOR DE COBRANZAS		
16	1106773731	QUIJANO GONZALEZ YENIT FERNANDA	ASESOR DE COBRANZAS		
17	80800771	RODRIGUEZ DIAZ CARLOS ESTEBAN	ASESOR DE COBRANZAS	INDEFINIDO	
18	39683699	RODRIGUEZ BERNAL MARIA DEL PILAR	ASESOR DE COBRANZAS	INDEFINIDO	
19	52620672	CANO CUBILLOS NANCY ESPERANZA	ASESOR DE COBRANZAS	Indefinido	
20	1010199263	RODRIGUEZ BURGOS MARIA FERNANDA	SUPERVISOR		
21	1073687352	ORTIZ HERNANDEZ HEIDER FABIAN	AUXILIAR OPERATIVO		
22	1026266315	RODRIGUEZ CUBILLOS YIVANA	ASESOR DE COBRANZAS T.F		
23	1030563375	MORENO CUBILLOS KATHERINE LISET	ASESOR DE COBRANZAS T.F	Fijo	
24	1031156499	LOPERA VARGAS ESTEPHANIE ALEJ	ASESOR DE COBRANZAS	FIJO	
25	1030646249	FLORIANO SON ANGIE KATHERINE	ASESOR DE COBRANZAS T.F	FIJO	
26	1020798435	ZANKO RINCON SANTIAGO	ASESOR DE COBRANZAS T.F	FIJO	
27	1000804415	BELMONTE LISPKI BRAYAN STID	ASESOR DE COBRANZAS T.F	FIJO	
28	1014292445	ULLOA ARDILA PAULA VANESSA	ASESOR DE COBRANZAS T.F	FIJO	
	1026286315	Yivana Andrea Rodriguez Cubillos	Asesor de Cobranzas	FIJO	
30	1.030.606.442	Fernandez Ramos Alexander	Visitador		Vesador Fernandez
	80800771	Esteban			

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOC

REGIONAL: Beta U/cio **FECHA:** 04-05 [illegible]

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	86.051.915	William Cordoba Machado	Auxiliar Administrativo	Indefinido	
2	11413576	Johann Cuyet Moros Lopez	Abogado Interno	Indefinido	
3	1121859434	Angel C. Gomez Ruiz.	Asesor cobranza.	INDEFINIDO	
4	1121876545	Jonathan L. Gallego Obando	Asesor	Indefinido	
5	40389896	Andrea Castaño Rincon	Asesor	Indefinido	
6	1121937130	Michel Daniela Gonzalez Quintero.	Asesor	Temporal	
7	1121832666	LAURA LIZETH ZAPATA CAUPAS	ASESOR	INDEFINIDO	
8	1121877548	Shirley Catherine Arcilla	Asesor.	Fijo	
9	1121891116	Hector Hilton Bermudez Almanza	Asesor	Fijo	
10	1121.878.101	Jorge Mauricio Suarez	Asesor	Fijo	
11	40367024	Maria Ingia Rodriguez Ortiz	Director	indefinido	
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					

Página 1

DEPARTAMENTO DE CAPACITACIÓN Y DESARROLLO COBRANZAS BETA

NOMBRE DEL CURSO Ingeniería Social.

HORARIO | **FECHA** 03/05/2017.

REGIONAL VALLEDUPAR

Con mi firma en esta relación certifico que recibí, comprendí y aplicaré la información.

N°	NOMBRE	CARGO	COMPAÑÍA	FIRMA
1065830010	Jeison Caldera Ponton	Gestor Cobranza	Promotora y Cobranza Beta	
1121328814	[illegible]	Asesora Comercial	Beta S.A	
49761729	[illegible]	Asesora Comercial	Beta S.A	
1065585381	[illegible]	Visitadora	Beta	
1065616750	[illegible]	Asesora	Beta	
1790131	[illegible]	Aux. Operativo	Beta	
37324326	[illegible]	Director	Beta	
7571865	[illegible]	Abogado	Beta	

OBSERVACIONES

- *Pishing
- *Baiting
- *Pretexting
- *Dumpster Diving
- *Shoulder
- *Tailgating
- *Cyber bulling
- *Happy slapping

- Scating
- Sextorsión
- Grooming

* Recomendaciones: Conciencia
  - No aceptar personas desconocidas.
  - Cuidado con la inf. q/ publicamos

* Reporte Área de Sistemas
  Seguridadtic@cobranzasbeta.com.co
  Vsplantacion: 602, 603, 609

G.7 Lista de asistencia 7

ACTA

VIDEO CAPACITACIÓN INGENIERÍ SOCIAL

Por medio de la cual se da inicio a ver el video de Cpacacitación Ingeniería Social:

- ¿Qué es la Ingeneria Social?
- Diferentes técnicas de la Ingeneria Social
- Técnicas más comunes de la Ingeneria Social
- ¿Cómo detectar diferentes formas de Ingeneria Social?
- ¿Cómo evitar las diferentes técnicas de ataques de Ingeneria Social?

ASISTENTES

MARIBEL ALVAREZ MONTEJO.....
Directora Oficina

MARILU CORDERO MORALES.....
Auxiliar Operativo

ANDREA VICTORIA GAMBOA AYURE.....
Asesora de Cobranzas

NIDIA PATRICIA LARA ESPINOSA.....
Asesora de Cobranzas

FLOR ALBA VIVAS PACATEQUE.....
Asesora de Cobranzas

KEILA YARLÑEDY ORDOÑEZ RAMIRES.....
Asesora de Cobranzas

ANGELA PAOLA DIAZ GAMEZ.....
Asesora de Cobranzas

DANIEL FERNANDO PORRAS PRIETO.....
Asesora de Cobranzas

JOSE ALVARO FORERO MENDOZA.....
Asesora de Cobranzas

En constancia de lo anterior se firma a los 02 dias del mes de mayo de 2017 en la oficina de Promociones y Cobranzas Beta S.A. Tunja.

G.8 Lista de asistencia 8

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL

REGIONAL: SANTA MARTA **FECHA:** 23/04/2017

N°.	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	7143007	JOSE LUIS JIMENEZ RODRIGUEZ	ASESOR VISITADOR	FIJO	
2	1082935724	JEISON JAIR PEREZ CANIZARES	ASESOR	FIJO	
3	1082853890	NADIA ISABEL GUERRA CASTILLO	ASESOR	INDEFINIDO	
4	1082905655	ANGELICA MARIA JIMENEZ SAMPAYO	ASESOR	INDEFINIDO	
5	57435758	ROSIRIS MEZA DE HUGUETT	ASESOR	INDEFINIDO	
6	49741063	MARTHA PATRICIA KERGUELEN JOHNSON	ASESOR	INDEFINIDO	
7	55221155	KATHERINE MILENA SANTAREN GUTIERREZ	ABOGADO INTERNO	INDEFINIDO	
8	36562744	FABIOLA SANCHEZ MARTINEZ	AUXILIAR ADMINISTRATIVO	INDEFINIDO	
9	8533797	RAMON ENRIQUE GARCIA DIAZGRANADOS	DIRECTOR REGIONAL	INDEFINIDO	
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					

Página 1

G.9 Lista de asistencia 9

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL:BETA- PASTO FECHA: 05/05/2017

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	98.389.109	JUAN PABLO CASTILLO ESPAÑA	DIRECTOR JURIDICO	T.I	
2	1.085.289.025	LEIDY JOHANA DELGADO NICHOY	AUXILIAR OPERATIVO	T.I	
3	87.068.833	ROSERO PABON CHRISTIAN	ASESOR COBRANZAS	T.I	
4	12.751.822	MOLINA GAVIRIA DANNY	ASESOR COBRANZAS	T.I	
5	1.085.283.144	ALAN MOSQUERA JIMENEZ	ASESOR COBRANZAS	T.F	
6	1.085.287.410	JUAN DAVID ACOSTA ORTEGA	ABOGADO INTERNO	T.F	

G.10 Lista de asistencia 10

CAPACITACION Y DESARROLLO

NOMBRE DEL CURSO CAPACITACION INGENIERIA SOCIAL

FECHA MAYO 4 DE 2017 HORA : 5:00 P.M.

No.	C.C.	NOMBRE	CARGO	FIRMA
1	7730036	Carlos Mauricio Cerquera Losada	Director	
2	12117835	Luis Fernando Gòmez Suarez	Asesor	
3	1075210836	Sandra Milena Diaz Roa	Asesora	
4	1144067303	Carlos Enrique Rivera Ramòn	Visitador	
5	1077863997	Ingrid Lorena Lugo Cabrera	Asesora	
6	36313149	Diana Paola Triviño Garzòn	Asesora	
7	1075224614	Carlos Arturo Bautista Hernandez	Asesor	
8	36310844	Sulman Paola Pulido Pulido	Asesora	
9	1075252189	Maria del Mar Mèndez Bonilla	Abogada Interna	
10	36171871	Emèrita Cuenca Andrade	Auxiliar Administrativa	

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: MONTERIA **FECHA:** 04/04/2017

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1067878887	Cindy Ibáñez Mesa	Abogada	Indefinido	
2	50'926.614	Maria Luisa Diaz R	Asesor Visitador	Indefinido	
3	26.201574	DINA Bucharo Pelo	Aux. Cobranzas	Indefinido	Dina Bucharo R.
4	26000404	Glen Racero Otero	Aux Operativa	Indefinido	Glen Racero
5	11'004.963	Jhony Javier Hoyos C	Asesor Cobranzas	Indefinido	Jhony J. Hoyos C.
6	50.916.553	Edith Oviedo C.	Asesor Cobranza	Indefinido	Edith Oviedo C
7	1064 197 897	ANGELA RAMOS DIAZ	ASESOR DE COBRO	FIJO	ANGELA RAMOS D.
8					
9					
10					
11					
12					
13					
14					
15					

Página 1

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: MEDELLIN **FECHA:** **02/05/2017**

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1017129234	Wilson Sarith Ochoa	Supervisor	Indefinido	
2	43.478.079	Alba Patricia Gutierrez G.	Asesora	Indefinido	
3	1.091-457-946	Leidy Johanna Bayona Tetuan	Recepcion.	Indefinido	Leidy Bayona.
4	43628568	Lina Ma Gaviria Gomez	Abogada	Indefinido	Lina Ma Gaviria G.
5	1020446706	Luisa Fernanda Monsalve Cano	Auxiliar Operativo	Fijo	Luisa Fernanda Monsalve C.
6	43125503	Maria Victoria Gaviria	Asesor comercial	Indefinido	
7	42.126.536	Luz Estella Ochoa G.	" "	Indefinido	
8	1039139859	Paola Andrea Gonzalez	Asesora	Indefinido	Paola Gonzalez
9	1039139859	Yuly Andrea Gil	Asesora	Fijo	Yuly Andrea Gil
10	43555574	Maria Isabel Arboleda	Asesor comercial	Indefinido	Maria Isabel Arboleda
11	1152471836	Liceth Tatiana Gonzalez Rodriguez	Asesor.	Fijo.	
12	1017170294	Didi Sanchez Tapias	Asesora.	Fijo.	Didi Sanchez
13	1039639474	Nayiber Dayana Salas Montoya	Asesora.	Fijo.	Nayiber Dayana Salas.
14	1036662941	Jessica Alejandra Carvajal E.	Asesora	Indefinido	Jessica Carvajal
15	1152451314	Juliana Monsalve Marin	Asesor.	Indefinido	Juliana Monsalve
16	94376629	Jhon Camilo Gomez A.	" " "	Indefinido	
17	1020428251	Juan Esteban Gonzalez S.	" " "	INDEFINIDO	
18	71.762.761	Wilson Gomez Toro	Asesor	Indefinido	
19	1037508686	Shirley Angel	Asesora	Fijo	Shirley Angel
20	91743830	Ruben Dario Alvarez G.	Asesor	INDEFINIDO	Ruben Dario Alvarez G.
21	1152450234	Santiago Hincapie Hincapie	Asesor	Fijo	Santiago H. H.
22	1039139897	Andres Mauricio Ocampo G.	Asesor	Fijo	Andres Ocampo
23	1017191607	Maria Melisa Velasquez B.	Asesora	Indefinido	Melisa Velasquez
24	1128289068	Leidy Johana Ochoa Suarez	Asesora	INDEFINIDO	Leidy Johana Ochoa O.
25	1129279636	Ingrid Briyith Cartagena	Asesora	Indefinido	
26	1039200865	Ana Maria Rivera O.	Asesora	Indefinido	Ana Maria Rivera O.
27	1035478048	Daniel Hernandez	Asesor	Fijo	
28	43074134	Maria Leticia Anaya	Directora	Indefinido	
29					
30					
31					
32					
33					
34					
35					
36					

Página 1

G.13 Lista de asistencia 13

Promociones y Cobranzas Reis S.A.

TEMA CAPACITACIÓN: INGENIERIA SOCIAL

CIUDAD: MANIZALES

LISTA DE ASISTENCIA

APELLIDOS Y NOMBRE	CEDULA	CARGO	FIRMA
JUAN CARLOS GRAND MARIN	10.263.760	Director Regional	
FRANCIA ELENA MARÍN JARAMILLO	24.341.701	Abogada interna	Francia E. Marin J.
FRANCIA MÓNICA PALACIO BADILLO	30.403.430	Asesora de Cobranzas	Mónica Palacio
LLAINI SOLANLLE PINEDA LONDOÑO	30.236.586	Asesora de Cobranzas	
CARLOS ANDRÉS HINCAPIÉ BERRIO	8.439.855	Asesor de Cobranzas	
VIVIANA ANDREA RIVERA GARZÓN	1.053.819.149	Asesor de Cobranzas	
JULIANA ANDREA PÉREZ MARTÍNEZ	1.053.824.059	Asesor de Cobranzas	VACACIONES
YURY ALEXANDRA LÓPEZ SÁNCHEZ	1.031.154.606	Asesor de Cobranzas	Y. Alexandra López.
YENNY ANDREA AGUDELO ALVAREZ	1.060.649.606	Asesora de Cobranzas	Agudelo.
HÉCTOR RICARDO CALLE VALLEJO	75.078.492	Auxiliar Operativo	

G.14 Lista de asistencia 14

Promociones y Cobranzas Beta S.A.

Regional

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: IBAGUE FECHA: 04/09/207

Nº	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	79.671.278	HERNAN MAURICIO RIVEROS QUEVEDO	DIRECTOR REGIONAL	T.I.	
2	1.110.484.883	ANGELA ROCIO SALAZAR GIRALDO	AUXILIAR ADMINISTRATIVO	T.I.	
3	65.776.603	ADRIANA YULIETH CASTELLANOS MORENO	ASESOR FRONT	T.I.	
4	1.104.701.496	BERLY LICETH RIOS ORTEGON	ASESOR COBRANZA	T.I.	
5	93.411.133	FELIX ESTEBAN TALERO ALVAREZ	ASESOR VISITADOR	T.F.	
6	1.110.477.713	ELIZABETH VARON HERNANDEZ	ASESOR COBRANZA	T.I.	
7	65.784.950	PAOLA ANDREA GARCIA ROJAS	ASESOR COBRANZA	T.I.	
8	1.104.708.197	DANIELA RODRIGUEZ HUERTAS	ASESOR COBRANZA	T.I.	
9	1.110.504.785	JORGE ANDRES ARCILA ROBLEDO	ABOGADO INTERNO	T.I.	
10	1.110.525.361	JULIAN DAVID AUDANA CASTRO	ASESOR COBRANZA	T.F.	
11	1.129.522.147	ANA YAMILE NEUTA RODRIGUEZ	ASESOR COBRANZA	T.F.	
12	1.110.459.911	KATHERIN ANDREA CORRALES ORTIZ	ASESOR COBRANZA	T.I.	
13	1.110.523.146	MIGUEL ANGEL ARCINEGAS BERNAL	DEPENDIENTE JUDICIAL	T.F.	
14	1.110.534.675	LAURA CATALINA RODRIGUEZ NIETO	ASESOR COBRANZA	T.F.	
15					

Página 1

G.15 Lista de asistencia 15

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: CÚCUTA FECHA: 06/06/2017

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	60450916	LEYDA ROCIO RIOS C	Asesora Cobranzas	Indefinido	
2	1004049339	Yoselin Lorena Quintero	Asesora Cobranza	NASES	
3	1004827851	Mayerling Yulieth Mayorga	Asesora cobranzas	FIJO	
4	1093224166	Ingrid Dayana Taraldo Sanchez	Asesora cobranzas	fijo	
5	1093752427	Sindy Julieth Alcedo Portillo	Asesora Cobranzas	Indefinido	
6	37.293.551	Jandi Lineth Cardenas Parra	Asesora cobranzas	INDEFINIDO	
7	1004041010	Sandra Lyliana Rodriguez G.	Asesora Cobranza	fijo	
8	60391366	SANDRA M GONZALEZ P.	ASESOR DE ACTIVO	INDEFINIDO	
9	60391640	Elizabeth Rodriguez Rodriguez	Abogada	Indefinido	
10	37449405	Jennifer C Ortiz Peñaloza	Aux. Operativo	Indefinido	
11	1004053574	Francisco Suarez ojeda	dependiente tecnico	Fijo	
12	1093745085	Yicsel Eudeny Rios Neira	Asesora Judicial	Indefinido	
13					
14					
15					
16					
17					
18					
19					
20					

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: Cartagena **FECHA:** 03/03/2017

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	33333914	[illegible]	[illegible]	[illegible]	[illegible]
2	45555806	Karen Barón	Asesora de Cobranzas	Indefinido	
3	1128053446	Luz M. Luna R.	Asesora de cobranzas	fijo	
4	1143338038	Martin Alfredo Puerta	Asesora de cobranzas	obra labor	Martin Alfredo
5	33311970	Gloria M. Romero S	Abogada	Indefinido	
6	64552934	Jenny Hollmoz	Asesora de Cobranza.	Indefinido	
7	45 510948.	Yenis Ardila Escobar.	Asesora de Cobranza.	Indefinido	
8	45545058	Matty Marquez Pinzon	Asesor de Cobranza	Indefinido	
9	73370975	Rafael Ovedo B	Asesor de cobranza	Indefinido	
10	1047443074	Jessica Ramos Mendoza	Aux Administrativo	Indefinido	
11	45.494.460	Yamil Luna Cataleta	OVK Operativo	Indefinido	Yamil Luna C.
12	78743742	Juan C. Arrieta C.	Visitador	indefinido	Juan C. Arrieta.
13	45505763	Daira Galvis Puerta	Asesora Cobranzas	Indefinido	Daira G
14	45765506	Yetty palomino Santoya	Asesor cobranzas.	Indefinido	Yetty P
15					
16					
17					
18					
19					
20					
21					

Página 1

G.17 Lista de asistencia 17

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL

REGIONAL:BETA CALI FECHA: 06/05/2017

Nº	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1[illegible]53	Gustavo Payan	Supervisor	Indefinido	
2	2[illegible]65	Jenny Tatiana Acosta	Asesora de Cobranzas	Indefinido	
3	2[illegible]45	Angelica Maria [illegible]	Asesora de cobranzas	Indefinido	
4	1[illegible]85	Stefania Ospina Tabima	Asesora Cobranzas	Fijo	
5	1[illegible]206	Jessica Amaya	Asesora Cobranzas	Fijo	
6	1.144.149.032	Mayra Ariza	Auditora Cobranzas	Fijo	
7	6[illegible]600	Mabel Hernandez	Asesora	Indefinido	
8	[illegible]	[illegible]	Aseora	Fijo	
9	1[illegible]098	Diana Milena Borrero Lucumi	Asesora de Cobranzas	Fijo	
10	2[illegible]	[illegible]	Asesora de cobranzas	Fijo	
11	1[illegible]48	[illegible]	Asesora de cobranzas	Fijo	
12	[illegible]	[illegible]	Asesora de cobranzas	Fijo	
13	[illegible]	[illegible]	Asesora Cobranzas	Fijo	
14	1[illegible]005	[illegible]	Asesora Cobranzas	Fijo	
15	1[illegible]017	Angela Francisca [illegible]	Auxiliar Operativo	Indefinido	
16	1[illegible]27	Edwin Valencia	Asistente	Indefinido	
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					

Página 1

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: BUCARAMANGA **FECHA:** **10/05/2017**

N°	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	40018231	Clara Susana Salcedo Espinosa	Directora Regional	Indefinido	
2	1098647278	Jaime Andres Mojica Prada	Supervisor	Indefinido	
3	1095809884	Alver Leonardo Muñoz Vanegas	Asesor	Termino Fijo	
4	37925586	Balbina Macias Castro	Asesor	Indefinido	
5	1098797515	Miguel Angel Pabon Rincon	Asesor	Termino Fijo	
6	63321535	Elsa Pedraza Rangel	Asesor	Indefinido	
7	37556845	Luz Milena Ortiz Moreno	Abogada Interna	Indefinido	
8	1098728310	Gina Daniela Arévalo Rodriguez	Asesor	Termino Fijo	
9	63494780	Claudia Juliana Sanchez Baron	Asesor	Indefinido	
10	27988474	Fanny Mogollon Afanador	Asesor	Indefinido	
11	1098622546	Yuli Paola Ariza	Asesor	Indefinido	
12	1095817690	Juan Sebastian Murillo Bedoya	Asesor	Indefinido	
13	91538354	Otniel Campo Barrero	Visitador	Indefinido	
14	91184137	Nelson Rodriguez Plata	Auxiliar Operativo	Indefinido	
15	13720616	Henry Duvian Cepeda Gutierrez	Asesor	Indefinido	
16	1095919822	Diana Viviana Rincon Caceres	Asesor	Indefinido	
17	1098698317	Blanca Yesenia Bermudez Romero	Dependiente	Termino Fijo	
18	63549405	Astrid Rocio Ramirez Silgado	Aprendiz Sena	Aprendiz SENA	

G.19 Lista de asistencia 19

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: Barranquilla **FECHA:** **02/05/2017**

Nº	CEDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
1	1140891221	Sharon Lopez Martinez	Asesor	Fijo	
2	72004658	Jean Carlos Gomez Quintero	Asesor	Fijo	
3	72202151	Arturo De Diego	Asesor	Independiente	
4	8628502	Patricia Mercado F	Asesor	Independiente	
5	22741602	Katherine Zarate R	Asesor	Fijo	
6	1226014772	Yenni Mirlanda Barrios	Telemercadista - Cobro	Independiente	
7	32339344	Karen Tatiana Martinez	Asesor	Independiente	
8	32860820	Adriana Maldonado A.	Auxiliar	FIJO	
9	85206091	Jesus Urango Urango	Abogado	Independiente	
10	8838392	Jeronimo Gonzalez C.	Cobrador	Independiente	
11	32282035	Nubia Dorado	Cobro de Cartera	Fijo	
12	32855905	Elvia Cecilia Rodriguez	Asesor Recaudo	Independiente	
13	32862291	Karen Patricia Montes	Director Regional	Independiente	
14	32867410	Yaneth Chaparro	Dir Administrativo	Independiente	
15	22531695	Jacqueline Rojas Guillen	Aux Administrativo	Independiente	
16	72302402	Jenni Milena Moreno P.	Asesor	Fijo	
17	1143954777	Cristian Leandro Romero	Auxiliar Sena	Fijo	
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					

Página 1

G.20 Lista de asistencia 20

Regional

Promociones y Cobranzas Beta S.A.

LISTA ASISTENCIA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE LA INGENIERÍA SOCIAL.

REGIONAL: ARMENIA **FECHA:** 27/03/2017

	CÉDULA	FUNCIONARIO	CARGO	CONTRATO	FIRMA
	41907227	DORALBA MARIN LUNA	DIRECTOR REGIONAL	INDEFINIDO	
	1094886664	DIANA MAGALY HERNANDEZ MONTOYA	AUXILIAR ADMINISTRATIVO/OPERATIVO	INDEFINIDO	
	24587135	LINA PATRICIA SUESCUN NARANJO	ABOGADA	INDEFINIDO	
	24587135	DIANA JOHANNA VALENCIA SALAMANCA	DEPENDIENTE JUDICIAL	FIJO	
	41962764	LORENA MARIA RODRIGUEZ GONZALEZ	ASESOR COBRANZAS	INDEFINIDO	
	1094934612	JUAN SEBASTIAN CARDONA OROZCO	ASESOR COBRANZAS	INDEFINIDO	
	1094951262	JESSICA ALEJANDRA PEREZ ALARCON	ASESOR COBRANZAS	FIJO	
	41958032	BIBIANA CONSUELO MONTOYA RUIZ	VISITADOR	INDEFINIDO	

Página 1

Anexo H. Manual presentación concientización Ingeniería Social Beta